Cybersecurity Roles and Functions Taxonomy
5 sources
The source provides a comprehensive outline of various careers within the cybersecurity field, organizing them by function. It categorizes roles into three primary areas: **Defensive Roles (Blue Team)**, which focus on monitoring and incident response; **Offensive Roles (Red Team)**, which involve ethical hacking and testing system defenses; and **Governance, Risk & Compliance (GRC) Roles**, which concentrate on strategy and adherence to security standards. Additionally, the text lists **Specialized & Emerging Roles**, such as Digital Forensics Analysts and Cryptographers, and notes several **Entry-Level & Supporting Roles** that provide foundational experience. This framework offers a clear understanding of the diverse responsibilities and specializations available within the industry, ranging from executive leadership to technical analysis.

How do different cybersecurity functions—offensive, defensive, and GRC—interact strategically?
The strategic interaction among Offensive, Defensive, and Governance, Risk, and Compliance (GRC) functions forms a critical feedback loop essential for maintaining an organization's overall security posture.
These three functions work together to identify threats, protect assets, manage risk, and ensure alignment with organizational strategy and regulatory requirements.
1. GRC and Strategic Oversight
The GRC function provides the **strategic backbone** for the organization's cybersecurity efforts, ensuring that defensive and offensive activities align with business objectives and risk tolerance.
• **Executive Leadership and Strategy:** Roles like the Chief Information Security Officer (CISO), who falls under the GRC category, act as the executive leader responsible for the **overall cybersecurity strategy**. The CISO and other senior executives are often business people with an understanding of risk management, rather than being exclusively chief hackers.
• **Risk Management and Decision-Making:** GRC roles involve working at a high level with decision-makers, including audit and risk committees, CIOs, and sometimes CEOs. They identify, assess, and mitigate cybersecurity risks to the organization.
• **Architectural Strategy:** Security Architects, who often engage in long-term planning and designing end-to-end security solutions, plan, research, and design a **robust security infrastructure** within a company.
2. Defensive and GRC Interaction
The Defensive team (Blue Team), typically centered around the Security Operations Center (SOC), executes the daily protection and response duties, providing crucial operational data back to the GRC function for strategic evaluation.
• **Risk Reporting and Compliance:** SOC analysts and teams are required to report on risks to the GRC team. This feedback loop is essential for GRC professionals to understand the current threat landscape and compliance gaps.
• **Management Oversight:** The SOC Manager, who supervises the security operations team, reports to the CISO (a GRC role) or other top-level management positions. SOC managers also support security audits.

• **Documentation and Improvement:** SOC analysts create detailed documentation and reports on security incidents, procedures, and risk assessments for senior management and stakeholders. This documentation aids GRC in assessing and improving the organization's security defenses. GRC guidelines also ensure that compliance regulations are met.

3. Offensive and Defensive Feedback Loop

The Offensive team (Red Team or penetration testers) strategically interacts with the Defensive team by emulating real-world attacks to validate and improve existing protective measures.

• **Testing and Validation:** Offensive roles, such as penetration testers, legally attempt to breach systems to find vulnerabilities *before* malicious actors do. Red Teamers emulate real-world attackers to test an organization's security defenses.

• **Vulnerability Identification and Improvement:** Highly experienced Defensive personnel, such as Tier 3 Threat Hunters, perform or supervise **vulnerability assessments and penetration tests** to identify possible attack vectors. This integration ensures that the Defensive team learns directly from successful breach attempts and recommends ways to optimize deployed security monitoring tools.

• **Continuous Enhancement:** Security Architects, who are responsible for designing secure systems, conduct regular system and vulnerability tests and implement or supervise the implementation of enhancements.

In essence, **GRC** defines *what* must be protected and *why* (governance, risk appetite); the **Offensive** team tests *how* easily the controls can be bypassed; and the **Defensive** team implements the controls, monitors for threats, responds to incidents, and reports back on the operational risks identified through monitoring and offensive testing.

The interaction among these functions is like a system of checks and balances where GRC sets the policy (the blueprint of a secure fortress), the Defensive team mans the walls and monitors the gates (the operations), and the Offensive team constantly tries to find weak spots in the walls and gates to ensure they hold up against real adversaries (quality assurance).

What essential skills and responsibilities define the diverse cybersecurity roles outlined in the source?

The diverse roles within cybersecurity are often categorized into five main areas: Defensive Operations, Offensive Operations, Security Engineering and Architecture, Governance Risk and Compliance (GRC), and Strategic and Leadership roles.

Here is a breakdown of the essential skills and responsibilities that define these diverse cybersecurity roles:

---

1. Defensive Operations (Blue Team)

Defensive roles focus on implementing protection measures, monitoring systems, and responding to incidents.

Role	Key Responsibilities	Essential Skills & Activities

Security Analyst / SOC Analyst	**Monitors security systems, detects threats, and responds to incidents**. Key duties include security monitoring, alert triage (determining priority and handling false positives), incident detection, investigation, and response. They manage security tools (like SIEM and IDS/IPS) and integrate threat intelligence.	**Analytic and critical thinking skills**. Strong understanding of cybersecurity principles and technologies. Familiarity with cybersecurity frameworks. Requires handling variety, such as responding to fishing, malware, or user access problems.
Tier 1 — Triage Specialist	Mainly responsible for **collecting raw data** and reviewing alarms and alerts. They confirm, determine, or adjust the criticality of alerts, enrich them with relevant data, and identify whether an alert is justified or a false positive. They prioritize and escalate issues to Tier 2 if unresolved.	Skills related to managing and configuring monitoring tools.
Tier 2 — Incident Responder	Reviews higher-priority security incidents escalated from Tier 1. They perform **in-depth assessment** using threat intelligence and must understand the scope of the attack and affected systems. They are responsible for designing and implementing strategies for containment and recovery.	Ability to transform raw attack telemetry data into actionable threat intelligence.

Tier 3 — Threat Hunter	The most experienced workforce in a SOC. They handle major incidents escalated by incident responders. **Most important responsibility is proactively identifying possible threats, security gaps, and vulnerabilities that might be unknown**. They may also perform or supervise penetration tests and vulnerability assessments.	Deep technical knowledge and expertise in reviewing critical security data and recommending optimization for monitoring tools. Proactively searches for advanced threats that bypassed existing controls.
Security Administrator	**Manages and maintains security infrastructure and access controls**.	Requires foundational IT skills (often starting as an IT Technician/Network Engineer).
Cloud Security Engineer	**Secures cloud-based applications and infrastructure**.	Specialized knowledge in cloud environments.
DevSecOps Engineer	Integrates security into the software development lifecycle (SDLC).	Knowledge of both security practices and software development.

---

2. Offensive Operations (Red Team & Adversary Emulation)
Offensive roles legally test an organization's systems by emulating real-world attackers.

Role	Key Responsibilities	Essential Skills & Activities

Penetration Tester / Ethical Hacker	**Legally attempts to breach systems to find vulnerabilities** before malicious actors can exploit them. They hack into a company to find weaknesses, create a report detailing those weaknesses, and help the company fix them.	Must **study constantly** to stay on top of all new hacks, techniques, and tools. This work requires high technical demands.
Red Teamer	**Emulates real-world attackers** to test an organization's security defenses.	Adversary emulation techniques.
Malware Analyst / Reverse Engineer	Studies malicious software (malware) to **understand its behavior** and create countermeasures. Provides support by reverse engineering malware to inform incident investigations and threat intelligence.	Highly technical skills in analyzing advanced threats and research. Computer forensics and malware analysis skills.
Vulnerability Researcher/Exploit Developer	Identifies system weaknesses and develops methods to exploit those weaknesses.	Highly specialized technical skills in finding and exploiting flaws.

---

3. Engineering and Architecture Roles
These roles focus on designing, building, automating, and maintaining the secure technology infrastructure.

Role	Key Responsibilities	Essential Skills & Activities

Security Architect	**Designs and builds secure IT systems and infrastructure**. They are involved in long-term planning and looking at the security posture end-to-end. They plan, research, and design robust security infrastructure, conduct regular system/vulnerability tests, and establish recovery procedures.	Day-to-day activities often involve meetings, research, and creating documents, spreadsheets, and PowerPoint presentations. Requires extensive experience in cybersecurity.
Cyber Security Engineer	A tools specialist; this role can encompass many areas, such as network security engineer (managing firewalls/proxies), cloud security engineer, or Identity and Access Management engineer (configuring tools like Sailpoint or CyberArk). They may also be automation specialists who write Python scripts to automate tasks.	Requires a foundational technical knowledge, such as being a proficient network engineer. They focus on building tools.
Cryptographer	Develops and implements cryptographic techniques to secure data.	Specialized knowledge in cryptography.

---

4. Governance, Risk, and Compliance (GRC) Roles
GRC roles typically involve non-technical tasks focusing on regulatory frameworks, risk management, and assessments.

Role	Key Responsibilities	Essential Skills & Activities

GRC Analyst/Specialist	Performs **risk analysis and compliance analysis**, writes reports, and conducts assessments. They need to understand how risk management and cybersecurity frameworks work. This is often a non-technical role, meaning they don't configure tools, but they must understand what the tools do and why they are needed.	Understanding of organizational risk and compliance requirements. Involves working with various teams, auditors, and senior management. This specialization often offers the **best work-life balance**.
Security Auditor / IT Auditor	**Assesses systems against security standards** and identifies compliance gaps.	Knowledge of security standards and compliance regulations.
Risk Manager	Identifies, assesses, and mitigates cybersecurity risks to the organization.	Expertise in risk identification and mitigation strategies.
Security Consultant	Researches security standards and best practices, compares current security operations capabilities, and assists in planning and designing security architectures.	Strong research and analytical skills concerning industry standards.

---

5. Strategic and Leadership Roles

These roles involve managing personnel, setting organizational strategy, and overseeing financial aspects of security.

Role	Key Responsibilities	Essential Skills & Activities

CISO (Chief Information Security Officer)	The **executive leader responsible for the overall cybersecurity strategy**. At the highest level, they are often business people with a deep understanding of risk management, rather than strictly technical experts.	Strategic thinking, risk management expertise, and reporting to top-level management.
SOC Manager	**Supervises the security operations team**. Responsibilities include hiring, training, and evaluating team members; creating processes; assessing incident reports; and developing crisis communication plans. They also oversee financial aspects and support security audits.	Leadership, team management, and strategic oversight.
Cyber Security Manager	Refers to all leadership roles, such as managers of small teams, people managers, or directors. They may manage technical teams (like penetration testers) or GRC professionals.	Requires strategic thinking, managing people and technology, and report writing.

Specialized & Supporting Roles
Other crucial specialized roles include:
• **Digital Forensics Analyst (Forensics Specialist):** Investigates cybercrimes by analyzing digital evidence, which can include memory, hard drives, or mobile devices. This role involves tight timelines and high-pressure deliverables.
• **Vulnerability Manager:** Continually identifies, assesses, reports on, manages, and remediates vulnerabilities across systems and endpoints.
• **OSINT Investigator/Analyst:** Gathers and analyzes open-source intelligence to identify threats.
The fundamental difference in many cybersecurity careers can be viewed like a supply chain: GRC determines the standards (the blueprints), Architects design the security systems (the

factory layout), Engineers build and maintain the tools (the machinery), and Analysts and Incident Responders monitor and fix problems as they arise (the operations team).

How are specialized and emerging cybersecurity roles adapting to evolving technological threat landscapes?

Specialized and emerging cybersecurity roles are adapting to evolving technological threat landscapes by integrating security into development processes, adopting advanced technical analysis techniques, focusing heavily on strategic design, and leveraging automation to handle complexity.

The adaptation of these roles focuses on specific areas of the technological landscape:

1. Integrating Security into Modern Technologies

The rise of cloud environments and rapid software development methodologies necessitate specialized roles that bake security into the infrastructure and development life cycle:

• **Cloud Security Engineer:** This role specializes in securing cloud-based applications and the underlying infrastructure.

• **DevSecOps Engineer:** These professionals integrate security directly into the software development lifecycle, ensuring that protection measures are implemented early in the process.

• **Security Architect:** A Security Architect must design and build secure IT systems and infrastructure. They perform long-term planning and look at the cyber security environment end-to-end. Their work involves planning, researching, and designing robust security infrastructure.

2. Proactive Defense and Advanced Analysis

As threats become more sophisticated and harder to detect, specialized roles focus on hunting hidden issues and deeply analyzing malicious techniques:

• **Threat Hunter:** This role proactively searches (hunts) for advanced threats that may have bypassed existing security controls. Threat hunters, often corresponding to Tier 3 analysts in a Security Operations Center (SOC) structure, proactively identify possible threats, security gaps, and vulnerabilities that might be unknown to the organization. They also review security data and recommend ways to optimize deployed security monitoring tools.

• **Malware Analyst/Reverse Engineer:** These specialists offer support in responding to sophisticated threats by reverse engineering malware to understand its behavior and create countermeasures. This work informs incident investigations and helps improve future detection and response efforts.

• **Vulnerability Researcher/Exploit Developer:** These specialists adapt to new weaknesses by identifying system vulnerabilities and developing the methods necessary to exploit them.

• **OSINT Investigator/Analyst:** This role is focused on gathering and analyzing open-source intelligence to identify threats, showing an adaptation toward leveraging publicly available information for defense.

• **Digital Forensics Analyst:** These analysts are crucial during incident response as they investigate cyber events or crimes by analyzing digital evidence, such as compromised machines, memory, or hard drives, to determine what truly occurred.

3. Leveraging Automation and Engineering

To effectively manage the complexity and massive scale of data generated by modern IT environments, security teams are augmenting human analysts with technology:

• **Automation:** The human element remains the most critical factor in a successful SOC, but automation and machine learning are leveraged to augment and complement human skills.
• **Accelerating Response:** Advanced analytics and AI significantly reduce the time teams spend processing massive amounts of data, providing critical security insights. Automation accelerates incident investigations by handling repeatable, low-level tasks and orchestrating actions across the product stack, enabling faster and more scalable Incident Response (IR).
• **Security Engineers:** While the title can vary, some Security Engineers specialize as **automation specialists** who write scripts (like Python scripts) to automate certain processes within security teams, such as the SOC, GRC, or offensive operations.
4. Strategic Governance and Risk Management
Highly strategic and leadership roles, often grouped under Governance, Risk, and Compliance (GRC), adapt by focusing on organizational strategy rather than just technical implementation:
• **Security Architect:** While highly technical, the architect role is strategic, ensuring the security design meets the organization's needs and establishes recovery procedures.
• **CISO (Chief Information Security Officer):** As the executive leader, the CISO is responsible for the overall cybersecurity strategy. These senior executive roles are focused on risk management and business understanding, often commanding high salaries due to their strategic impact.
• **Security Consultant:** Consultants often research security standards and best practices to provide an industry overview, helping organizations plan, research, and design robust security architectures to meet evolving needs.
The evolving nature of cyber threats requires **continuous improvement**. Security personnel, including analysts, engineers, and architects, must continuously adapt through training and retention efforts, while core roles like **SOC analysts** must consistently stay current with evolving cyber threats and trends to enhance their detection and prevention strategies.

The adaptation of specialized cybersecurity roles to technological threats is like a **biological immune system evolving against a rapidly mutating virus.** The core defense (SOC/Blue Team) handles the common infections, but the specialized cells (Threat Hunters, Malware Analysts, Security Architects, and DevSecOps Engineers) constantly study the new mutations, proactively seek out hidden threats, and redesign the genetic defenses (infrastructure and development processes) to make the host organization fundamentally resistant to the next generation of attack.
Are GRC jobs non-technical?
Based on the sources, Governance, Risk, and Compliance (GRC) jobs are typically **referred to as non-technical roles**, though this requires clarification regardingBased on the sources, Governance, Risk, and Compliance (GRC) jobs are typically **referred to as non-technical roles**, though this requires clarification regarding the necessary knowledge base.
Here is a breakdown of why GRC roles are characterized this way:
GRC Roles are Typically Non-Technical
GRC is a specialization that is generally considered non-technical because the primary responsibilities do not involve configuring or installing security tools.

• **Focus on Frameworks and Analysis:** GRC involves a group of roles where professionals perform tasks like **risk analysis** and **compliance analysis**, write reports, and conduct assessments.
• **Best Work-Life Balance:** GRC is considered the **best cybersecurity specialty for work-life balance** because the work is usually organized, typically a 9-to-5 job with no middle-of-the-night calls, as GRC personnel are not responsible for responding to cyber attacks.
• **High-Level Strategy:** GRC roles become increasingly high-level and strategic as professionals gain seniority, working with decision-makers such as audit and risk committees, CIOs, and sometimes CEOs. The CISO (Chief Information Security Officer), an executive leader responsible for overall cybersecurity strategy, falls under the GRC category and is often viewed as a **business person with an understanding of risk management**, rather than strictly a technical expert or "chief hacker".
Required Technical Understanding
While GRC professionals do not typically configure tools, they must still possess essential knowledge of the technical landscape:
• **Understanding Tools and Needs:** GRC specialists need to know **what tools like Splunk do and why they are needed**, even if they are not the person configuring them.
• **Framework Expertise:** They must understand **how risk management works** and be familiar with cybersecurity frameworks, why they are necessary, and how they function.
• **Security Architecture Overlap:** Highly experienced GRC-related roles, such as the **Security Architect**, who designs secure solutions and performs long-term planning, fall under GRC but require extensive cybersecurity experience due to the high-impact decisions they make.
In summary, GRC roles are non-technical in their day-to-day execution (less hacking and coding, more documents, spreadsheets, and meetings), but they require a **strategic and foundational understanding of technology, risk management, and cybersecurity principles** to effectively guide the organization's security posture.
What are offensive security roles?
Offensive security roles, often categorized as the **Red Team** or **Adversary Emulation**, focus on legally testing an organization's systems by thinkingOffensive security roles, often categorized as the **Red Team** or **Adversary Emulation**, focus on legally testing an organization's systems by thinking and acting like real-world attackers to find and address weaknesses before malicious actors exploit them.
In the analyzed dataset, Offensive Operations was identified as one of the five main categories used to classify cybersecurity jobs. These roles generally demand high technical skills and include specialized titles.
Here is a breakdown of the roles and key characteristics associated with offensive security:
Key Offensive Security Roles
The sources outline several roles that fall under the Offensive Operations category:
• **Penetration Tester (Ethical Hacker):** This role involves legally attempting to breach systems to find vulnerabilities. Ethical hackers hack into a company to identify weaknesses, generate a report detailing those weaknesses, and help the company fix them. Penetration testers must constantly study to stay current with all new hacks, techniques, and tools due to the high technical demands of the work.

• **Red Teamer:** This is a general term for specialists who emulate real-world attackers to test an organization's security defenses.
• **Vulnerability Researcher/Exploit Developer:** These specialists identify system weaknesses and develop methods to exploit them.
• **Malware Analyst (Reverse Engineer):** This role involves studying malicious software (malware) to understand its behavior and create countermeasures. Malware Analysts or Reverse Engineers offer support in responding to sophisticated threats by reverse engineering malware to inform incident investigations, provide threat intelligence, and improve future detection and response efforts.
The analysis of 100 job postings categorized Offensive Operations with three standardized titles:
1. **Cyber Intelligence Analyst**
2. **Exploitation Operations Specialist**
3. **Reverse Engineer Specialist**
In the job data analyzed, there were only six jobs classified as offensive security/penetration tester type roles out of 100 job listings, suggesting this specialization has a relatively low number of job openings compared to defensive or engineering roles.
Work Life Balance and Technical Demands
Offensive roles often require significant dedication and may impact work-life balance due to the nature of the work:
• **Non-Standard Hours:** Ethical hacking activities often occur after working hours or on weekends to avoid interrupting mission-critical systems during business hours.
• **Continuous Study:** Ethical hackers need to study constantly to keep up with new hacks, techniques, and tools, which places high technical demands on the individual.
• **Enjoyment:** People who are passionate about ethical hacking tend to enjoy it significantly, often engaging in hacking projects as a hobby outside of work.
Career Path and Salary
Offensive security roles are generally not considered beginner-friendly:
• **Entry-Level Availability:** Ethical hacking is statistically one of the worst jobs to pursue as an entry-level candidate because most roles demand significant technical experience, advanced certifications (like OCP), and high-level technical skills. Most cybersecurity professionals do not typically start in ethical hacking. Similarly, roles like **security researcher** and **malware reverse engineer** are typically senior roles, not entry-level positions.
• **Salary:** While all cybersecurity jobs pay well, some sources suggest that penetration testing or ethical hacking may not pay the "best" when compared to other specializations, given the high effort and skill required. However, the raw data analysis showed that offensive security roles, along with leadership roles, tended to be among those with the **highest salaries** when sorting by average compensation (up to approximately $228,000 in the sample). This potentially reflects that the advertised salaries are skewed toward mid-to-senior level positions seeking experienced individuals.
For many advanced technical roles, such as Threat Analyst or Malware Reverse Engineer, individuals are often expected to have a lot of experience and usually start in roles like SOC analysts or ethical hackers before moving into specialized security research.
Which job has most openings?

Based on the analysis presented in the sources, the job that appears to have the most openings varies depending on whether you are looking at broad categories or specific standardized job titles.

Most Frequent Job by Standardized Title

The analysis of 100 cybersecurity job postings from Indeed, categorized using Python and the ChatGPT API, suggested that the role with the **most openings** based on standardized titles was **Security Architect**.

• **Security Architect** accounted for **20** of the 100 jobs analyzed.
  ◦ It is noted that the employer might have used a different title, but based on the job description, the analysis determined these jobs were actually for a Security Architect.

• The number two job with the most openings was the **Cyber Detection Engineer**, which the source suggests might be a variation of a **SOC Analyst**.

Most Frequent Job by Category and Entry-Level Availability

When looking at the five major categories (Offensive, Strategic/Leadership, GRC, Security Engineering, and Defensive Operations), the data showed that Defensive Operations, Security Engineering, and GRC jobs had a similar, larger share of the openings, while Offensive Security had the fewest.

• **Defensive Operations** and **Security Engineering** jobs had "quite a bit more" jobs available compared to Offensive Security, which had the least amount.

• **Offensive Security** jobs, such as Penetration Tester, accounted for only **six** of the 100 jobs.

Furthermore, when considering roles specifically suitable for entry-level candidates, two specializations were highlighted as having high availability:

1. **SOC Analyst (Security Operations Center Analyst):** This is considered **one of the best roles for an entry-level cyber security candidate** because there are "so many" SOC Analyst roles available compared to other specialties.
2. **GRC (Governance, Risk, and Compliance):** This specialization also has significant entry-level availability, making it an "absolute secret weapon" for landing a first job. GRC is described as not being just one role, but a group of roles including risk analysis, compliance analysis, and audit.

In contrast, roles like **Ethical Hacking (Penetration Tester)** are cited as one of the **worst jobs to do as an entry-level candidate** because there are not many of those jobs available, and most require advanced experience or technical certifications. Similarly, the highly specialized roles of **Threat Analyst/Security Researcher** and **Security Architect** are typically **not entry-level jobs**.

Therefore, while the specific raw data suggested **Security Architect** had the highest count (20), if you are looking for an accessible starting point, **SOC Analyst** and **GRC roles** are generally considered to have the largest number of entry-level job opportunities.

Which jobs pay the most?

Based on the raw data analysis and expert commentary provided in the sources, the jobs that tend to pay the most fall into the categories of **Strategic/Leadership rolesBased on the raw data analysis and expert commentary provided in the sources, the jobs that tend to pay the most fall into the categories of **Strategic/Leadership roles** and **Offensive Operations**, particularly those requiring high levels of experience and strategic responsibility.

Here is a breakdown of the highest-paying roles according to the sources:

1. Highest Paying Categories (Based on Data Sample)

An analysis of 100 job postings from Indeed, where salaries were visible, revealed that jobs categorized under Offensive Operations and Strategic/Leadership roles generally commanded the highest average compensation:

• **Offensive Security:** This category, which includes roles like Exploitation Operations Specialist and Reverse Engineer Specialist, showed a high average salary of approximately **$228,000**.

◦ The source suggests this high average might be because the salaries listed on platforms like Indeed tend to be for more **mid-to-senior level roles** seeking experienced individuals.

• **Leadership/Strategic Roles:** When sorting the standardized job titles by highest salary, offensive security and leadership type roles (red and orange heavy) were prominently featured at the top of the list.

2. Roles Paying the Most Money

Specific job titles identified as paying the most, particularly at senior levels, include:

• **Security Architect:** This role, which involves designing solutions and long-term planning for the end-to-end security posture, is recognized as one of the jobs that **pays the most money**. This is because it is performed by individuals with significant experience who bring substantial value and impact to the business.

• **Chief Information Security Officer (CISO):** The CISO is the executive leader responsible for the overall cybersecurity strategy. At the **highest level** of GRC and leadership, such as for global banks, senior executives (like CISOs) have been known to receive salaries close to **seven figures** when bonuses are factored in, though this is not typical. These executive roles are primarily business roles focused on risk management, not technical hacking.

• **Cyber Security Manager (Leadership Roles):** Generally, roles with more responsibility, such as management positions (including managing technology, people, or multiple teams), typically correspond to **more money**. Planning to get into management is suggested if maximizing salary is a top priority.

3. Comparison with Other Roles

While most cybersecurity jobs pay well, some roles are explicitly noted as paying less on average compared to the most strategic or highly technical specializations:

• **GRC Roles:** Generally, GRC roles pay well, and salaries increase significantly at the senior level (e.g., CISO).

• **Offensive Security (Penetration Testing):** Although penetration testing appeared high in the raw data analysis, some experts feel that, given the amount of effort and skill required, ethical hacking and penetration testing "don't really pay the best" compared to other cybersecurity jobs, though they still pay a lot of money overall.

• **Threat Analyst/Security Researcher/Malware Reverse Engineer:** These highly technical senior roles, while essential, are often described as having **average salaries** in local organizations when compared to the highest-paying specializations, although highly senior roles at large tech companies (like Google or Microsoft) pay extremely well.

• **SOC Analyst:** On the junior level, SOC analysts will **not pay the best**, but there is significant upward potential, allowing progression to roles like SOC Manager or Principal Incident Responder, which command higher salaries.

• **Digital Forensics Analyst:** The money for this specialization is **not that high** compared to others, though it is still good at senior levels.

• **Cyber Security Engineer:** Salaries for general engineering roles are often described as **average**.

In summary, the highest salaries are reserved for roles that blend deep experience with executive decision-making (CISO, Security Architect) or require rare, advanced offensive technical skills (Exploitation Specialist, Reverse Engineer Specialist).

What are the job categories?

Based on the analysis of 100 job postings and general descriptions of cybersecurity functions provided in the sources, the jobs are generally classified into **five main categories**:

1. **Defensive Operations (Blue Team)**: These roles focus on implementing protection measures, monitoring security systems, detecting threats, and responding to incidents. Examples include SOC Analyst, Incident Responder, and Security Administrator.
2. **Offensive Operations (Red Team & Adversary Emulation)**: These roles legally attempt to breach systems and find vulnerabilities before malicious actors do, often emulating real-world attackers. Examples include Penetration Tester (Ethical Hacker), Red Teamer, and Vulnerability Researcher.
3. **Security Engineering and Architecture**: This category involves jobs focused on designing, building, automating, and maintaining the secure technology infrastructure. Examples include Security Architect, Cyber Security Engineer, and Cryptographer.
4. **GRC (Governance, Risk, and Compliance) Jobs**: These roles involve non-technical tasks focusing on regulatory frameworks, risk management, compliance analysis, and assessments. Examples include CISO, Security Auditor, and Risk Manager.
5. **Strategic and Leadership Jobs**: These roles are management-type roles that involve supervising teams, setting organizational strategy, and overseeing financial aspects of security. Examples include CISO (also categorized in GRC), SOC Manager, and Cyber Security Manager.

These categories were developed to analyze job descriptions, determine which job types have the most openings, and identify which job types pay the most. After categorizing the 100 raw job listings into these five groups, the roles were further broken down into standardized job titles for more specific analysis.

Who is a Security Architect?

A **Security Architect (SA)** is a specialized and senior role focused on the strategic design and planning of an organization's secure IT systems and infrastructure.

Here is a detailed breakdown of the Security Architect role based on the sources:

Core Responsibilities and Function

The Security Architect is primarily responsible for ensuring that the organization's technology landscape is robustly secured from an end-to-end perspective.

• **Design and Planning:** The SA's main duty is to **plan, research, and design a robust security infrastructure** within a company. They are involved in long-term planning, looking at the cybersecurity environment end-to-end.

• **System Testing and Enhancement:** They are expected to conduct **regular system and vulnerability tests**. They also implement or supervise the implementation of enhancements to the security infrastructure.

• **Establishing Recovery Procedures:** Security Architects are responsible for **establishing recovery procedures** to ensure the organization can recover from incidents.

• **Strategic Oversight:** This role involves designing security solutions and making decisions that impact the security posture of the entire organization and the daily work of the cybersecurity team.

Classification and Seniority

The Security Architect role is placed strategically within the organizational structure:

• **Category:** It is categorized under **Security Engineering and Architecture**, and is also considered a **Specialized & Emerging Role**.

• **GRC Overlap:** While primarily an architecture role, it **falls under Governance, Risk, and Compliance (GRC)** because it focuses on high-level design and risk decisions.

• **Seniority and Experience:** This is **not an entry-level job**. It is a senior role that one must aspire to after spending years working in cybersecurity. The decisions they make require significant experience in cybersecurity.

Daily Work and Work-Life Balance

The nature of the Security Architect's work is highly strategic and less hands-on with tools:

• **Work-Life Balance:** The Security Architect enjoys **one of the best work-life balances** in cybersecurity, similar to other GRC jobs. It is typically a 9-to-5 job, and they are generally not the person who gets called at 3:00 a.m. when things go wrong.

• **Daily Activities:** The day-to-day job often consists of strategic and documentation tasks, including:

  ◦ Meetings
  ◦ Google research
  ◦ Creating Word documents
  ◦ Preparing PowerPoint presentations
  ◦ Working with Excel spreadsheets

• **Contrast to Technical Roles:** If a person prefers hacking, coding, or being "in the tools," the Security Architect role is **not for them**. The work is not characterized by "hoodies and hacking and blinking lights".

Job Market and Compensation

The Security Architect role is highly valued in the job market:

• **Job Availability:** In an analysis of 100 job postings, **Security Architect** had the **most openings** available compared to other standardized titles, accounting for **20** of the jobs.

• **Salary:** This is one of the jobs that **pays the most money**. The high salary reflects the amount of experience required and the significant value and impact they bring to the business.

SECURE YOURSELF

PROTECT YOUR DATA