Resources for video:

* <https://www.varonis.com/blog/cybersecurity-careers/>
* <https://medium.com/@coderacademy/10-careers-in-cyber-security-you-should-consider-2613061a8cb2>

Careers:

* Security Researcher
  + <https://cybersecurity.att.com/blogs/security-essentials/the-life-of-a-security-researcher>
  + <https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html> - case study type deal
  + Malware Analyst
    - <https://blog.malwarebytes.com/security-world/2012/09/so-you-want-to-be-a-malware-analyst/#:~:text=What%20is%20a%20Malware%20Analyst,also%20how%20it%20does%20it>.
  + Cryptographer
    - <https://www.cybersecurityeducation.org/careers/cryptographer/>
  + Threat Researcher
  + Vulnerability Researcher
    - Strong background in systems programming (low level stuff), this knowledge can be obtained outside of university- though may be more of a challenge.
* Penetration Tester
  + Physical Pen-tester
  + Network Pen-tester
* SOC Analyst
  + https://blog.eccouncil.org/soc-analysts-what-they-are-what-they-do-and-why-they-matter%E2%80%AF/
* NOC Analyst and Network Security Engineer
  + https://www.fieldengineer.com/skills/noc-analyst
* Security Engineer
* Software Tester (Security/Code Auditor)
  + <https://www.clearlaunch.com/code-audit/>
  + I.T. Auditor
* Cyber Security Consultant
* CISO
  + https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html
* Computer Forensics Analyst
* Security Architect
* Incident Responder
* Sysadmin
* Nation-state hacker

Components:

* What they do
* Average salary
* Certifications and education level
* Transferable Skills
* Career paths
* Similar jobs and overlap between jobs

Video Format:

* Group jobs based on what you do
* Group by tier (entry, mid, advanced)

Template

Q. What do you do?

A.

Q. Where do you work?

A.

Q. What’s the pay range?

A.

Q. Common Certifications and Degrees

A.

Q. Potentially Transferable Skills

A.

Q. Related Jobs

A.

Q. Links and Related Resources

A.

Penetration Tester

Q. What do you do?

A. Network: Sit at a computer and attempt to break into devices on the network using known vulnerabilities and exploits. This includes five stages: Information Gathering, Vulnerability Analysis, Exploitation, Privilege Escalation, and Post-Exploitation (though many consider post-exploitation an umbrella term and lump privilege escalation underneath it)

Info Gathering: learning about the company, scanning and analysing components on the network

Vulnerability Analysis: determining ways in or vulnerabilities in the services on the network components

Exploitation: leveraging those vulnerabilities to obtain a shell (terminal window) that allows unauthorized interaction with other network components

Privilege Escalation: Attempting to gain greater privileges (Administrator or root) after already having access to a machine

Post-Exploitation: Obtaining passwords, logging keystrokes, taking screenshots, pass-the-hash, leveraging machine to gain access to others in its network

Physical: Very little demand

Q. Where do you work?

A. Depends on the environment. May work from home, in an office, at the site of the company being pen tested.

ex. ScienceSoft, Acunetix, Netsparker, CyberHunter, ImmuniWeb, HackerOne, FireEye, Rapid7, BreachLock, CloudStrike, Offensive Security (OffSec)

Q. What’s the pay range?

A. $60k to $170k

ZipRecruiter claims national average at $116k

CyberSeek claims average at $104k

PayScale claims $85k

Q. Common Certifications and Degrees

A. EC-Council Certified Ethical Hacker (CEH) and Licensed Penetration Tester (LPT)

Information Assurance Certification Review Board (IACRB) Certified Penetration Tester (CPT) or Certified Expert Penetration Tester (CEPT) or Certified Red Teams Operations Professional (CRTOP)

CompTIA PenTest+

Offensive Security Certified Professional (OSCP)

Global Information Assurance Certification (GIAC) Penetration Tester (GPEN) or Exploit Researcher and Advanced Penetration Tester (GXPN)

B.S. or M.S. in Cybersecurity Engineering

B.S. or M.S. in Computer Engineering

B.S. or M.S. in Computer Science

B.S. or M.S. in Information Technology

Q. Potentially Transferable Skills

A. Penetration testing tools and tactics, understanding of security vulnerabilities and how to mitigate them

Q. Related Jobs

A. IT Auditor, Cybersecurity Architect

Q. Links and Related Resources

* <https://www.cyberdegrees.org/jobs/penetration-tester/>
* <https://onlinedegrees.sandiego.edu/best-jobs-in-cyber-security/>
* [https://resources.infosecinstitute.com/topic/top-5-penetration-testing-certifications-security-professionals](https://resources.infosecinstitute.com/topic/top-5-penetration-testing-certifications-security-professionals/)
* <https://www.ziprecruiter.com/Salaries/Penetration-Tester-Salary>
* <https://www.payscale.com/research/US/Job=Penetration_Tester/Salary>
* <https://www.softwaretestinghelp.com/penetration-testing-company/>
* <https://cybersecurityventures.com/10-hot-penetration-testing-companies-to-watch-in-2020/>

System Administrator

Q. What do you do?

A.

* Keep track of all hardware and software
* Install updates and patches regularly
* Monitor CPU and memory utilization
* Oversee backups of all relevant data in case of a breach
* Harden machines, configure firewall rules, create user accounts and privileges
* Install and manage a syslog server for event logging in case of a breach
* Train new sysadmins if senior sysadmin

Q. Where do you work?

A. Typically at the company of hire, directly/remotely accessing their computers or speaking with other employees.

Q. What’s the pay range?

A. $40k to $90k

Average of $84k according to Indeed

$63k according to PayScale

Do it for a long time ⇒ become senior sysadmin which pays more

Q. Common Certifications and Degrees

A. Microsoft Certified Solutions Expert (MCSE), Oracle Linux System Administrator, Red Hat Certified System Administrator (RHCSA), Red Hat Certified Engineer (RHCE), CompTIA Server+, VMware Certified Professional, Linux Professional Institute (LPIC) System Administrator, ServiceNow Certified System Administrator

B.S. or M.S. in IT/Network Administration

B.S. or M.S. in Computer Science

B.S. or M.S. in Computer Engineering

Q. Potentially Transferable Skills

A. Very applicable to other cybersecurity or IT jobs, especially IT consultant or system architect

Service installation and management knowledge comes in handy for most jobs

* Database administration
* Network administration
* Security administration
* System analysis
* Cloud technology
* Programming
* Project management

Q. Related Jobs

* Senior Sysadmin
* Security Architect
* Security Consultant

Q. Links and Related Resources

* <https://www.fieldengineer.com/skills/what-is-a-system-administrator>
* <https://www.indeed.com/career/salaries/system%20administrator?from=acme-keyword-salaries&rawkeyword=System+Administrator&keyword=system+administrator&reason=indexedserp_url>
* <https://www.payscale.com/research/US/Job=Systems_Administrator/Salary>
* <https://www.degreequery.com/degree-need-systems-administrator/>
* <https://blog.netwrix.com/2018/07/19/best-system-administrator-certifications-for-2018/>
* <https://study.com/articles/How_to_Become_a_System_Administrator_Career_Roadmap.html>
* <https://www.newhorizons.com/article/4-career-paths-for-system-administrators-and-the-certifications-you-need-to-succeed>

Security Researcher

Q. What do you do?

A. You perform research on vulnerabilities, malware, threat actors and basically anything security related. For example security researcher Ian Beer spends his days researching vulnerabilities in Iphones and apple products. He monitors updates, leaks and alarms to try and find new and powerful vulnerabilities. One of his latest findings was a “wormable radio-proximity exploit which allowed him to gain complete control over any iPhone in his vicinity” (<https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html>). A lot of that work involves reverse engineering, exploit development and of course good old fashioned research! Malware research is really its own field (Malware Analysis) these guys reverse engineer malware to understand how it works, what exploits it might use and who made it among many other things. There is also the budding field of academic Security Research where Professors try to find ways to solve the ever increasing problems related to computer security. Academics may research better ways to secure everything from the Blockchain and Smart Contracts to Iot, and they try to find better ways to perform fuzzing, symbolic execution and many many more cool topics. Again these things don’t aren’t only studied by Academic researchers, there are many other people working on these problems, academics among them. Finally there are also threat intelligence researchers, who identify potential cyber threats for companies and organizations. So to summarize “Security Researcher” is more of an umbrella term that encompasses a number of job titles including vulnerability researcher, malware analyst, and even Professor. To close this is not an exhaustive list, but these are some of the common positions found under the umbrella of security researcher.

Q. Where do you work?

A. Google Project Zero, AlienVault Labs, Microsoft, Trustwave, Proofpoint, CISA, NSA|CSS, CIA, Fireye, Crowdstrike, Wells Fargo, Raytheon, Carbon Black, NCC Group, Zscaler, Oracle, Cofense, Mandiant, Lockheed Martin, Paypal, Nike, Carnegie Mellon (or any school that does sec research) Invictus, Pueo

Q. What’s the pay range?

A. According to payscale, base salaries can range from 61K-192K with an average of 122K

Q. Common Certifications, and Degrees?

A. So these are not super essential in this field and many people go their whole careers without any certifications, but the most applicable certifications that we could find were the GIAC Exploit Researcher and Advanced Penetration Tester (applicable for Vulnerability Researcher), GIAC Defending Advanced Threats (Threat Intelligence Analyst/Researcher). Applicable degrees may include anything in STEM, and sometimes people with other degrees can transition over (more self directed learning with this approach) or even people with no degrees. Common degrees include: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology

Q. Potentially transferable Skills?

A. Self directed learning, a solid understanding of computers and networks, and understanding of bleeding edge cybersecurity technologies, tools and tactics.

Q. Related Jobs?

A. Again since this is a bit of an umbrella term the jobs that are underneath the umbrella include: Vulnerability researcher, Malware Analyst/Researcher, Threat Intelligence Analyst/Researcher, Cryptographic Researcher, and General Cybersecurity Researcher.

Q. Some links and material tangentially related to this field?

* <https://www.sans.org/cyber-security-courses/?msc=main-nav>
* <https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html>
* <https://cybersecurity.att.com/blogs/security-essentials/the-life-of-a-security-researcher>
* <https://www.reddit.com/r/Malware/>
* <https://0x00sec.org/>

Cyber Forensic Analyst

Q. What do you do?

A. According to techtarget.com “Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law”. Essentially it’s like being a crime scene investigator, but the place that the crime to place is in CYBERSPACE. In all seriousness cyber forensic analysts typically follow a set of standardized procedures to ensure none of the original evidence was corrupted/contaminated. They make copies of the electronic storage devices and comb through those trying to pull out any evidence that may prove a suspect guilty of a cybercrime (or regular crime). The cases that cyber analysts are involved include: espionage, organized cybercrime, hacking, fraud, terrorism, and the storage and distribution of illegal content (cyberdegrees.org). In addition to understanding the technical aspects, a strong understanding of legal standards that guide investigations is also essential for cyber forensic analysts.

Q. Where do you work?

A. FBI, Booz Allen Hamilton, ManTech International Corporation, Air Force, various state Police, Northern Trust, PwC, CIA

Q. What’s the pay range?

A. $50K-$114K Range with average being about $74K (infosecinstitute.com)

Q. Common Certifications, and Degrees?

A.

* Certified Computer Forensic Examiner (CCFE)
* Certified Mobile Forensic Examiner (CMFE)
* Computer Hacking Forensic Investigator (CHFI)
* GIAC Certified Forensic Examiner (GCFE)
* GIAC Certified Forensic Analyst (GCFA)
* Certified Computer Examiner (CCE)

Degrees: Common degrees include: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology

Q. Potentially transferable Skills?

A. An understanding of how a hack was conducted requires strong technical knowledge that can be utilized in a number of different positions, from blue team to consultant. In addition the understanding of legal practices, and strong ethics are always a great thing to have in any business. In addition technology is ever evolving so as with most jobs in security, self directed learning is key to keep pace with technological evolution.

Q. Related Jobs?

A. Incident Response, Cybersecurity Consultant, Sysadmin

Q. Some links and material tangentially related to this field?

* <https://www.dhs.gov/science-and-technology/forensics>
* <https://searchsecurity.techtarget.com/definition/computer-forensics#:~:text=Computer%20forensics%20is%20the%20application,in%20a%20court%20of%20law>.
* <https://www.cyberdegrees.org/jobs/computer-forensics/>
* <https://resources.infosecinstitute.com/topic/average-forensic-computer-analyst-salary-2017/#:~:text=On%20average%2C%20forensic%20computer%20analysts,%2442%2C301%20to%20%24118%2C317%20each%20year>.
* <https://digital-forensics.sans.org/community/downloads>

Source Code Auditor

Q. What do you do?

A. Source Code auditor is a mid-tier job which generally requires a bit of experience in software engineering, web development and security. Source Code Auditors inspect source code of applications to try and spot vulnerabilities via their comprehensive analysis. In addition they try to spot bugs and syntax errors in the code that might interfere with normal use of the application. Source Code Auditors write many reports on their findings and give recommendations on the remediation of such bugs and errors. Source code auditors are key because they inspect source code with the mindset of a security professional (a mindset that may be lacking in developers, as there job is to produce working code, which isn’t always secure code) and try to analyze how might attackers leverage it to carry out attacks, this is where pentesting and general security knowledge combines with a robust understanding of software engineering. Source code auditors, may perform audits as part of a criminal investigation (like when a breach happens) or as part of a consultant gig. Source code auditors may also work in companies routinely combing through the code base for bugs.

Q. Where do you work?

A. Accenture, Verizon, Protocol Labs

Q. What’s the pay range?

1. On Average $66K (cybersecurityguide.org, payscale.com)

Q. Common Certifications, and Degrees?

A.

* Certified Information Systems Auditor (CISA)
* Offensive Security Certified Professional (OSCP)
* Offensive Security Experienced Penetration-tester (OSEP)
* Offensive Security Web Expert (OSWE)
* GIAC Certified Intrusion Analyst

Degrees: Common degrees include: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology

Q. Potentially transferable Skills?

A. Being able to communicate technical information to non-technical people (auditors may constantly communicate with lawyers who are typically not technical). Deep technical knowledge of programming and IT systems. An understanding of adversarial tactics (how hackers heck lol, no how they get in).

Q. Related Jobs?

A. Software Tester- with this job security is a critical component however the main focus is on quality assurance, and making the product works as intended. Software Engineer, Penetration Tester and Incident Response are all fields highly intertwined with Source code auditors because when there are vulnerabilities, specifically the high impact RCE one’s, they typically result in poorly written code. RCE’s are exploited by pentester, they’re “caused” by software engineers and cleaned up by Incident Response. Information Security Analyst and IT Auditor.

Q. Some links and material tangentially related to this field?

* <https://www.businessnewsdaily.com/10761-how-to-become-a-software-tester.html>
* <https://www.cyberdegrees.org/jobs/source-code-auditor/>
* <https://www.prospects.ac.uk/job-profiles/software-tester#:~:text=As%20a%20software%20tester%2C%20you,gets%20deployed%20to%20everyday%20users>.
* <https://www.cybersecurityeducation.org/careers/become-source-code-auditor/#:~:text=A%20source%20code%20auditor%20is,attack%20to%20test%20the%20code>.
* <https://infosecaddicts.com/career-path/why-and-how-to-become-a-source-code-auditor/>
* <https://cybersecurityguide.org/careers/security-code-auditor/>

Security Architect

Q. What do you do?

A. Obviously each company is different and so the specifics of what security architects do varies from company to company. With that being said in general this is a higher level position (below CISO but higher up the hierarchy than say an engineer) that involves quite a bit of strategy. To be more specific, security architects “work out how they (an organization) builds new policy, guidance and audit processes that enable the business to meet all of it’s security requirements”. Security architects leverage their deep technical knowledge to help structure an organization's security posture all the while keeping in mind business goals. Architects need to have a good understanding of vulnerabilities, system design, threats, risks, crypto, and be business savvy. A security generalist with a business twist. In addition to this SA’s oversee the testing of their environments (red team activities and formal pen-tests) and identify integration issues. Understanding a company's IT systems well is key.

Q. Where do you work?

A. Mantech, Geico, NVIDIA, Booz Allen Hamilton, Accenture, PNC Bank, Shure, SolarWinds (lol), Sophos, Walgreens, GitHub, Google, Cisco, Linkedin, Zoom, Verizon, Peloton, PepsiCo, Skechers

Q. What’s the pay range?

A. 89K-176K (payscale.com)

Q. Common Certifications and Degrees

A. As with all cyber careers this certs and degrees may help but are not necessary. Degrees: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology. Certs: Security+, Pentest+, OSCP, OSCE (certs are helpful to understanding security basics as opposed to directly applicable for this particular role).

Q. Potentially Transferable Skills

A. Deep technical knowledge of vulnerabilities, risk, distributed systems, pen-testing as well as the ability to work in tandem with different business units to accomplish goals are all highly sought after skills in the industry. Soft skills ie. breaking down technical concepts and report writing are also very transferable. Being able to manage others (since this is a bit of a management role is also very useful.

Q. Related Jobs

A. Consultant, Penetration tester, CISO, Cloud Architect

Q. Links and Related Resources

A.

* <https://medium.com/secjuice/what-is-a-security-architect-a65d3b0c9707>
* <https://www.careerexplorer.com/careers/security-architect/>
* <https://www.cyberdegrees.org/jobs/security-architect/>
* <https://www.infosecinstitute.com/career-profiles/security-architect/>
* <https://www.payscale.com/research/US/Job=Security_Architect/Salary>

Security Operations Center (SOC) Analyst

Q. What do you do?

A. Monitor network traffic and identify signs of malicious activity. Suggest improvements to mitigate/remediate cyber threats

Usually use a SIEM. When something potentially harmful is found, submit a ticket

May also check malicious IPs or files using a site that does this

Q. Where do you work?

A. For a company either in an office or remotely analysing logs

Q. What’s the pay range?

A. Generally $50k - $90k but up to $110k

Average of $76k according to glassdoor

$90k according to salary.com

$100k according to indeed

Q. Common Certifications and Degrees

* CompTIA CySA+
* CompTIA Sec+
* EC-Council Certified SOC Analyst (CSA)
* Cisco Certified CyberOps Associate

Q. Potentially Transferable Skills

* Network defense
* Penetration testing and evidence of this in logs
* Incident response
* Computer forensics
* Reverse engineering

Q. Related Jobs

* Threat Intelligence Analyst
* Vulnerability Analyst
* Cybersecurity Analyst
* Information Security Analyst/Administrator
* Security Administrator

Q. Links and Related Resources

* Highly recommended: <https://docs.google.com/presentation/d/1jtuRuVPhBRcNRjwtwS4BsAKP8696KfEZzojrPLDT4lk/edit?usp=sharing>
* <https://www.glassdoor.com/Salaries/soc-analyst-salary-SRCH_KO0,11.htm>
* <https://www.indeed.com/career/soc-analyst/salaries?hl=en>
* <https://www.salary.com/research/salary/listing/soc-analyst-salary>

Network Operations Center (NOC) Analyst

Q. What do you do?

A. Network troubleshooting, running diagnostics and securing the network, writing network infrastructure reports, replacing hardware, writing scripts for automating network operations, providing tech support, reviewing network logs

Q. Where do you work?

A. Typically at the company ⁠→ various locations depending on assigned task but mostly a desk job

Q. What’s the pay range?

A. $38k⁠–$71k with average at $54k according to glassdoor

$38k⁠–$63k with average at $50k according to salary.com

Q. Common Certifications and Degrees

A. B.S. or M.S. in CS, CE, IT, Cybersecurity

CCNP, CompTIA Network+, CompTIA Security+, CompTIA Cybersecurity Analyst (CySA+), MCSE

Q. Potentially Transferable Skills

* Understanding of computers
* Programming and scripting
* Customer service
* Communication
* Multitasking and time-management

Q. Related Jobs

A. Sysadmin, security architect

Q. Links and Related Resources

* <https://www.jobhero.com/job-description/examples/data-systems-administration/noc-analyst>
* <https://www.fieldengineer.com/skills/noc-analyst>
* <https://www.glassdoor.com/Salaries/noc-analyst-salary-SRCH_KO0,11.htm>
* <https://lensa.com/network-operations-center-noc-analyst-jobs/draper/jd/ba9016f6a70a7f51603ead1063cbd374>
* <https://www.fieldengineer.com/skills/network-security-operations-center-analyst>
* <https://www.comptia.org/blog/your-next-move-network-security-operations>

Security Engineer

Q. What do you do?

A. Secure a network environment

This includes testing and screening security software, hardening machines, monitoring the network for intrusion, assisting in responding to malicious threats, developing security standards and practices and providing security education to others

Q. Where do you work?

A. Generally at the company you work for in person directly or indirectly accessing the necessary machines

Q. What’s the pay range?

$52k - $84k according to glassdoor

$53k - $185k according to ziprecruiter with national average at $120k

$62k - $135k according to payscale with average at $92k

Average of $108k per year according to indeed

Q. Common Certifications and Degrees

A. Certified Information Systems Security Professional (CISSP) ⇒ must recertify every 3 years, Global Information Assurance Certification (GIAC), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH), Cisco Certified Network Professional Security (CCNP Security), GIAC Certified Incident Handler (GICH), GIAC Certified Intrusion Analyst (GCIA)

Degrees:

* Information Systems
* Information Technology
* Computer Science/Engineering
* Applied Mathematics

Q. Potentially Transferable Skills

* Penetration and vulnerability testing
* Firewall and intrusion detection/prevention protocols
* Windows, UNIX and Linux operating systems
* Virtualization
* MySQL/MSSQL database systems
* Application security and encryption
* Subnetting, DNS, encryption technologies and standards, VPNs, VLANs, VoIP and other network routing methods
* Network protocols
* Social engineering

Q. Related Jobs

A. SOC Analyst, Security Consultant, Security Architect, Sysadmin

Q. Links and Related Resources

* <https://www.careerexplorer.com/careers/security-engineer/>
* <https://www.ziprecruiter.com/Salaries/Cyber-Security-Engineer-Salary>
* <https://www.payscale.com/research/US/Job=Security_Engineer/Salary>
* <https://www.indeed.com/career/security-engineer/salaries>
* <https://www.glassdoor.com/Job/security-engineer-jobs-SRCH_KO0,17.htm>
* <https://www.fieldengineer.com/skills/information-security-engineer>
* <https://www.cyberdegrees.org/jobs/security-engineer/>
* <https://study.com/articles/information_security_engineer_certification_training_degree.html>

Incident Responder

Q. What do you do?

A. Incident Responders deal with a number of tasks relating to analyzing, triaging and dealing with cyber events. Obviously exact responsibilities will differ from company to company but in general you can think of incident responders similar to firefighters. When there is a breach or some kind of Incident, Responders typically get called in as part of a Security Incident Response Team (SIRT) to handle it. Incident Responders put policies and procedures in place to handle cyber events, and their jobs involve a lot of report writing (incident reports), investigating events/abnormalities and teamwork. When not in a crisis event IR are refining said policies and procedures as well as discussing security trends to stay one step ahead of the bad guys. These positions typically require a couple of years of experience in a field related to cyber forensics, system administration and etc. This job can be high stress as you can get called in at just about any time (24/7/365) and when you get called it’s usually because something has gone wrong.

Q. Where do you work?

A. Fireye, Transunion, KPMG, Blackberry, Marriott, Paypal, Red Canary, Aon, Secureworks, VISA, T-Mobile, SpaceX, Cisco, J.P. Morgan, HP, Verizon, RSM

Q. What’s the pay range?

A. Average is $69K, Ranges from $45K- $100K

Q. Common Certifications and Degrees

A. Common degrees include: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology.

Certs:

* GIAC Certified Incident Handler (GCIH)
* GIAC REsponse and Industrial Defence (GRID)
* Certified Information Systems Auditor (CISA)
* Offensive Security Certified Professional (OSCP)
* Offensive Security Experienced Penetration-tester (OSEP)
* Offensive Security Web Expert (OSWE)
* GIAC Certified Intrusion Analyst

Q. Potentially Transferable Skills

A. Deep technical knowledge of attacks, defenses and triage. Solid team skills, and an ability to perform under pressure. Effective communication is a skill needed to be successful in this field and is highly transferable to other positions.

Q. Related Jobs

A. SOC Analyst, Cyber Forensic Investigator, Sysadmin, Penetration Tester

Q. Links and Related Resources

A.

* <https://www.cyberdegrees.org/jobs/incident-responder/>
* <https://www.cybersecurityjobsite.com/job/5143414/senior-consultant-cybersecurity/>
* <https://www.cybersecurityeducation.org/careers/incident-responder/>
* <https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response/arming-your-incident-response-team>
* <https://infosecaddicts.com/career-path/why-and-how-to-become-an-incident-responder/>
* <https://infosecaddicts.com/career-path/why-and-how-to-become-an-incident-responder/>
* <https://www.glassdoor.com/Salaries/incident-response-salary-SRCH_KO0,17.htm>

Chief Information Security Officer (CISO)

Q. What do you do?

Head of the security operations. Oversees all security policies and procedures ⁠→ usually reports to Chief Information Officer (CIO) or directly to company CEO

* Real-time threat analysis
* Make sure staff doesn’t misuse data
* Security architecture
* User roles and access management
* Program management (system patches, education)
* Investigation and forensics in the event of an attack
* Making sure all initiatives run smoothly and are properly funded

Q. Where do you work?

A. At a company interacting with coworkers or directly accessing the available hardware

Q. What’s the pay range?

A. $83k to $221k with average at $160k according to ziprecruiter

$169k to $289k with average at $223k according to salary

$73k to $130k with average at $100k according to glassdoor

Q. Common Certifications and Degrees

* ⁠Certified Information Systems Security Professional (CISSP)
* Certified Information Security Manager (CISM)
* Certified Ethical Hacker (CEH)
* B.S. or M.S. in Computer Science/Engineering/ITM/related field

Q. Potentially Transferable Skills

* DNS
* Routing
* Authentication
* VPN
* Proxy services and DDOS mitigation
* Coding practices
* Ethical hacking
* Intrusion detection/prevention

Q. Related Jobs

A. CIO

Q. Links and Related Resources

* \*\*\* recommended: <https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html>
* <https://www.ziprecruiter.com/Salaries/Chief-Information-Security-Officer-Salary>
* <https://www.salary.com/research/salary/benchmark/chief-information-security-officer-salary>
* <https://www.glassdoor.com/Salaries/ciso-salary-SRCH_KO0,4.htm>
* <https://www.cybersecurityeducation.org/careers/chief-information-security-officer/>

Cybersecurity Consultant

Q. What do you do?

A. Consultants, at a high level, work with their organization or for a number of clients helping to secure them from cyber threats. They do this by analyzing the current infrastructure, proposing strategies to mitigate risks, delivering them to upper management and training employees to execute on the selected strategy. Consultants have a solid foundation of cybersecurity principles and they have a great understanding of how attackers operate and get in. Typically consultants will become specialists in one particular area of security. Specializations include: Cloud Security (google, aws, azure etc.), Incident Response, devops, etc. In general consultants are a bit like advisors for companies

Q. Where do you work?

A. Consulting firms usually. These include: PwC, Deloitte, Optiv, Cisco, Secureworks, Flashpoint, Cylance, FireEye, Accenture, IBM, IANS, Equilibrium IT Solutions, Myriad360, Dragos

Q. What’s the pay range?

A. Average $81K range $52K-$114K (glassdoor)

Q. Common Certifications and Degrees

A. Common degrees include: B.S. or M.S. in Cybersecurity Engineering, B.S. or M.S. in Computer Engineering, B.S. or M.S. in Computer Science, B.S. or M.S. in Information Technology. Note: certs will vary depending on your specialty

Certs:

* GIAC Certified Incident Handler (GCIH)
* GIAC REsponse and Industrial Defence (GRID)
* Certified Information Systems Auditor (CISA)
* Offensive Security Certified Professional (OSCP)
* Offensive Security Experienced Penetration-tester (OSEP)
* Offensive Security Web Expert (OSWE)
* GIAC Certified Intrusion Analyst
* AWS Certified Solutions Architect
* AZ-500 (Azure security)
* Google Cloud Professional Architect

Q. Potentially Transferable Skills

A. Highly developed technical knowledge in whatever their consulting specialty tends to be. The ability to communicate technical knowledge to non-technical people. Writing skills, as well as public speaking skills (presentations to boards of directors).

Q. Related Jobs

A. Cloud Security Architect, Incident Responder, Penetration Tester, CISO

Q. Links and Related Resources

A.

* <https://www.fieldengineer.com/skills/cyber-security-consultant>
* <https://www.ecpi.edu/blog/how-to-become-a-cyber-security-consultant>
* <https://www.bls.gov/careeroutlook/2018/interview/cybersecurity-consultant.htm>
* <https://builtin.com/cybersecurity/cyber-security-firms>
* <https://www.cyberdegrees.org/jobs/security-consultant/>
* <https://atlantsecurity.com/blog/>
* <https://www.careerexplorer.com/careers/it-security-consultant/>

Nation State Hacker

Q. What do you do?

A. Nation state hackers are usually part of a military/intelligence agency and serve to further the interests of the government that is backing them. They are extremely secret groups, and little is known about them other than they are some of the best scientists, hackers and operators on the planet and they have military budgets to back them. These groups are also known as advanced persistent threats or APT’s and typically they leave behind trademarks in their attacks that are used to correlate which attacks were performed by which APT. Working for a nation state hacking group you are performing attacks on other countries, examples of such attacks include: stuxnet, solarwinds, the shadow brokers attack, the ukraine power grid attack, operation aurora and many many more. The level of these attacks is highly sophisticated, and large teams are generally involved to execute them. Much of their work is shrouded in secrecy but it is an actual job in the industry, and it’s probably the most exciting one. Generally the most significant cyberattacks are conducted by these groups

Q. Where do you work?

A. American NSA, Russian GRU, Chinese PLU, Israel's Unit 8200

Q. What’s the pay range?

A. ???

Q. Common Certifications and Degrees

A.

Q. Potentially Transferable Skills

A. Everything mentioned above, this is pretty much the pinnacle of cybersecurity

Q. Related Jobs

A. Any of the previously mentioned jobs

Q. Links and Related Resources

A.

* <https://darknetdiaries.com/episode/28/>
* <https://darknetdiaries.com/episode/19/>
* <https://en.wikipedia.org/wiki/Advanced_persistent_threat#APT_groups>
* <https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html>
* <https://www.comparitech.com/blog/information-security/advanced-persistent-threat/>
* <https://www.fireeye.com/current-threats/apt-groups.html>