COOLEST CAREERS IN CYBER

SANS | GIAC CERTIFICATIONS

Organizations are hiring individuals with a unique set of skills and capabilities, and seek those who have the abilities and knowledge to fulfill many new job roles in the cybersecurity industry. The coolest careers in cybersecurity are the most in-demand by employers. Which jobs are the coolest and most in-demand? We know; let us show you the hottest cybersecurity jobs for 2023.

Curricula: Cyber Defense | Digital Forensics | Offensive Operations | Cybersecurity Leadership | Cloud Security | Industrial Control Systems | Purple Team

SEC460 GEVA ← GIAC Certification with course

01 Threat Hunter (Threat/Warning Analyst)

This expert applies new threat intelligence against existing evidence to identify attackers that have slipped through real-time detection mechanisms. The practice of threat hunting requires several skill sets, including threat intelligence, system and network forensics, and investigative development processes. This role transitions incident response from a purely reactive investigative process to a proactive one, uncovering adversaries or their footprints based on developing intelligence.

"Digging below what commercial anti-virus systems are able to detect to find embedded threat actors in client environments makes this job special. Shoutout to Malware and Threat Intelligence Analysts who contribute their expertise to make threat hunters more effective against adversaries."

- Ade Muhammed

Why is this role important?

Threat hunters proactively seek evidence of attackers that were not identified by traditional detection methods. Their discoveries often include latent adversaries that have been present for extended periods of time.

Recommended courses

FOR508 GCFA | FOR532 | FOR572 GNFA | FOR578 GCTI | FOR608 | FOR610 GREM | SEC497 GOSI | SEC504 GCIH | SEC541 GCTD | ICS515 GRID | ICS612

02 Red Teamer (Adversary Emulation Specialist)

In this role you will be challenged to look at problems and situations from the perspective of an adversary. The focus is on making the Blue Team better by testing and measuring the organization's detection and response policies, procedures, and technologies. This role includes performing adversary emulation, a type of Red Team exercise where the Red Team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries. It can also include creating custom implants and C2 frameworks to evade detection.

"The only way to test a full catalog of defense is to have a full catalog of offense measure its effectiveness. Security scanning is the bare minimum and having Red Team perform various operations from different points will help the organization fix weaknesses where it matters."

- Beeson Cho

Why is this role important?

This role is important to help answer the common question of "can that attack that brought down company, happen to us?" Red Teamers will have a holistic view of the organization's preparedness for a real, sophisticated attack by testing the defenders, not just the defenses.

Recommended courses

SEC504 GCIH | SEC542 GWAPT | SEC560 GPEN | SEC565 | SEC660 GXPN | SEC670 | SEC699 | SEC760

03 Digital Forensic (Cyber Defense Forensics Analyst)

This expert applies digital forensic skills to a plethora of media that encompass an investigation. The practice of being a digital forensic examiner requires several skill sets, including evidence collection, computer, smartphone, cloud, and network forensics, and an investigative mindset. These experts analyze compromised systems or digital media involved in an investigation that can be used to determine what really happened. Digital media contain footprints that physical forensic data and the crime scene may not include.

"Forensics is about diving deep into any system and device and locating the problem so as to develop a solution."

- Patricia M

"Data doesn't lie, and the digital forensic analyst looks at the data to convey the stories that they tell."

- Anthony Wo

Why is this role important?

You are the sleuth in the world of cybersecurity, searching computers, smartphones, cloud data, and networks for evidence in the wake of an incident/crime. The opportunity to learn never stops. Technology is always advancing, as is your career.

Recommended courses

FOR308 | FOR498 GBFA | FOR500 GCFE | FOR508 GCFA | FOR509 GCFR | FOR518 GIME | FOR532 | FOR572 GNFA | FOR585 GASF | SEC501 GCED

04 Purple Teamer

In this fairly recent job position, you have a keen understanding of both how cybersecurity defenses ("Blue Team") work and how adversaries operate ("Red Team"). During your day-to-day activities, you will organize and automate emulation of adversary techniques, highlight possible new log sources and use cases that help increase the detection coverage of the SOC, and propose security controls to improve resilience against the techniques. You will also work to help coordinate effective communication between traditional defensive and offensive roles.

"The combination of red team blue team operations is very interesting and you get to see both sides. I have been on a Purple Team for a while now and it has driven a lot of positive change for us."

- Andrew R

Why is this role important?

Help blue and red understand one another better! Blue Teams have traditionally been talking about security controls, log sources, use cases, etc. On the other side Red Teams traditionally talk about payloads, exploits, implants, etc. Help bridge the gap by ensuring red and blue are speaking a common language and can work together to improve the overall cybersecurity posture of the organization!

Recommended courses

SEC599 GDAT | SEC699 | SEC504 GCIH | SEC568 | SEC598

05 Malware Analyst

Malware analysts face attackers' capabilities head-on, ensuring the fastest and most effective response to and containment of a cyber-attack. You look deep inside malicious software to understand the nature of the threat – how it got in, what flaw it exploited, and what it has done, is trying to do, or has the potential to achieve.

"Being a malware analyst provides a great opportunity to pit your reverse engineering skills against the skills of malware authors who often do everything in their power to make the software as confusing as possible."

- Bob Pardee

Why is this role important?

If you're given a task to exhaustively characterize the capabilities of a piece of malicious code, you know you're facing a case of the utmost importance. Properly handling, disassembling, debugging, and analyzing binaries requires specific tools, techniques, and procedures and the knowledge of how to see through the code to its true functions. Reverse engineers possess these precious skills, and can be a tipping point in the favor of the investigators during incident response operations. Whether extracting critical signatures to aid in better detection, or producing threat intelligence to inform colleagues across an industry, malware analysts are an invaluable investigative resource.

Recommended courses

FOR518 GIME | FOR585 GASF | FOR610 GREM | FOR710 | SEC501 GCED

06 Chief Information Security Officer (CISO) (Executive Cyber Leadership)

The CISO leads staff in identifying, developing, implementing, and maintaining processes across the organization to reduce information and information technology risks. CISOs respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance, such as supervising efforts to achieve ISO/IEC 27001 certification for an entity or a part of it. Typically, the CISO's influence reaches the entire organization.

"The chief gets to coordinate the plans. The chief gets to know the team, know them well and disperse them appropriately to strategically defend and test org networks and security posture."

- Anastasia Edwards

Why is this role important?

The trend is for CISOs to have a strong balance of business acumen and technology knowledge in order to be up to speed on information security issues from a technical standpoint, understand how to implement security planning into the broader business objectives, and be able to build a longer lasting security and risk-based culture to protect the organization.

Recommended courses

MGT512 GSLC | MGT514 GSTRT | MGT516 | MGT520 | MGT521 | MGT551 GSOM | MGT553 | SEC566 GCCC | ICS418

07 Blue Teamer – All-Around Defender (Cyber Defense Analyst)

This job, which may have varying titles depending on the organization, is often characterized by the breadth of tasks and knowledge required. The all-around defender and Blue Teamer is the person who may be a primary security contact for a small organization, and must deal with engineering and architecture, incident triage and response, security tool administration and more.

"In this day and age, we need guys that are good at defense and understand how to harden systems."

- David O

Why is this role important?

This job role is highly important as it often shows up in small to mid-size organizations that do not have budget for a full-fledged security team with dedicated roles for each function. The all-around defender isn't necessarily an official job title as it is the scope of the defense work such defenders may do – a little bit of everything for everyone.

Recommended courses

SEC450 | SEC503 GCIA | SEC505 GCWN | SEC511 GMON | SEC530 GDSA | SEC555 GCDA | SEC586

08 Security Architect (NICE) and Engineer

Design, implement, and tune an effective combination of network-centric and data-centric controls to balance prevention, detection, and response. Security architects and engineers are capable of looking at an enterprise defense holistically and building security at every layer. They can balance business and technical requirements along with various security policies and procedures to implement defensible security architectures.

"A security architect needs to understand work flows, networks, business requirements, project plans and sometimes even budget restraints. A very diversified role!"

- Chris Bodill

Why is this role important?

A security architect and engineer is a versatile Blue Teamer and cyber defender who possesses an arsenal of skills to protect an organization's critical data, from the endpoint to the cloud, across networks and applications.

Recommended courses

SEC503 GCIA | SEC505 GCWN | SEC511 GMON | SEC530 GDSA | SEC549

09 Cyber Defense Incident Responder/Law Enforcement Counterintelligence Forensics Analyst

This dynamic and fast-paced role involves identifying, mitigating, and eradicating attackers while their operations are still unfolding.

"Incidents are bound to occur and it is important that we have people with the right skill set to manage and mitigate the loss to the organization from these incidents."

- Anita Ali

Why is this role important?

While preventing breaches is always the ultimate goal, one unwavering information security reality is that we must assume a sufficiently dedicated attacker will eventually be successful. Once it has been determined that a breach has occurred, incident responders are called into action to locate the attackers, minimize their ability to damage the victim, and ultimately remove them from the environment. This role requires quick thinking, solid technical and documentation skills, and the ability to adapt to attacker methodologies. Further, incident responders work as part of a team, with a wide variety of specializations. Ultimately, they must effectively convey their findings to audiences ranging from deep technical to executive management.

Recommended courses

FOR508 GCFA | FOR509 GCFR | FOR518 GIME | FOR532 | FOR572 GNFA | FOR578 GCTI | FOR608 | FOR610 GREM | FOR710 | SEC402 | ICS515 GRID | SEC504 GCIH

10 Cybersecurity Analyst/Engineer (Systems Security Analyst)

As this is one of the highest-paid jobs in the field, the skills required to master the responsibilities involved are advanced. You must be highly competent in threat detection, threat analysis, and threat protection. This is a vital role in preserving the security and integrity of an organization's data.

"It doesn't become much more versatile than in this role, as oftentimes you'll be challenged with whathever tasks or projects customers or managers envision, ranging from simple analysis support to introducing new solutions and implementing whole services such as a SOC."

- Harun Kuessner

Why is this role important?

This is a proactive role, creating contingency plans that the company will implement in case of a successful attack. Since cyber attackers are constantly using new tools and strategies, cybersecurity analysts/engineers must stay informed about the tools and techniques out there to mount a strong defense.

Recommended courses

SEC401 GSEC | SEC450 | SEC501 GCED | SEC503 GCIA | SEC530 GDSA | SEC555 GCDA | SEC504 GCIH | SEC554 | FOR508 GCFA | FOR509 GCFR | MGT551 GSOM | SEC510 GPCS | SEC540 GCSA | SEC549 | ICS410 GICSP | ICS456 GCIP

11 OSINT Investigator/Analyst

These resourceful professionals gather requirements from their customers and then, using open sources and mostly resources on the internet, collect data relevant to their investigation. They may research domains and IP addresses, businesses, people, issues, financial transactions, and other targets in their work. Their goals are to gather, analyze, and report their objective findings to their clients so that the clients might gain insight on a topic or issue prior to acting.

"Being an OSINT investigator allows me to extract information in unique and clever ways and I am never bored. One day I'm working on a fraud investigation and the next I'm trying to locate a missing person. This job always tests my capabilities, stretches my critical thinking skills, and lets me feel like I'm making a difference."

- Rebecca Ford

Why is this role important?

There is a massive amount of data that is accessible on the internet. The issue that many people have is that they do not understand how best to discover and harvest this data. OSINT investigators have the skills and resources to discover and obtain data from sources around the world. They support people in other areas of cybersecurity, intelligence, military, and business. They are the finders of things and the knowers of secrets.

Recommended courses

SEC497 GOSI | SEC587 | FOR578 GCTI

12 Technical Director (Information Systems Security Manager)

This expert defines the technological strategies in conjunction with development teams, assesses risk, establishes standards and procedures to measure progress, and participates in the creation and development of a strong team.

"A technical director must have strong cybersecurity knowledge, a strategic view of the organization's infrastructure and what's to come, and communication skills. These things are hard to get, and I would imagine this job to be very challenging, no matter the organization size or business."

- Francisco Lugo

Why is this role important?

With a wide range of technologies in use that require more time and knowledge to manage, a global shortage of cybersecurity talent, an unprecedented migration to cloud, and legal and regulatory compliance often increasing and complicating the matter more, a technical director plays a key role in successful operations of an organization.

Recommended courses

MGT512 GSLC | MGT514 GSTRT | MGT516 | MGT551 GSOM | SEC566 GCCC | ICS418

13 Cloud Security Analyst

The cloud security analyst is responsible for cloud security and day-to-day operations. This role contributes to the design, integration, and testing of tools for security management, recommends configuration improvements, assesses the overall cloud security posture of the organization, and provides technical expertise for organizational decision-making.

"This role is essential to find and patch vulnerabilities in the cloud environment to ensure that crackers and hackers are unauthorized in cloud environments."

- Ben Yee

Why is this role important?

With an unprecedented move from traditional on-premise solutions to the cloud, and a shortage of cloud security experts, this position helps an organization position itself thoughtfully and securely in a multicloud environment necessary for today's business world.

Recommended courses

SEC488 GCLD | SEC510 GPCS | SEC541 GCTD | SEC401 GSEC | FOR509 GCFR | SEC588 GCPN

14 Intrusion Detection/SOC Analyst (Cyber Defense Analyst)

Security Operations Center (SOC) analysts work alongside security engineers and SOC managers to implement prevention, detection, monitoring, and active response. Working closely with incident response teams, a SOC analyst will address security issues when detected, quickly and effectively. With an eye for detail and anomalies, these analysts see things most others miss.

"The intrusion analyst is the guard at the gate and can get great job satisfaction from detecting and stopping network intrusions."

- Chuck Ballard

Why is this role important?

SOC analysts help organizations have greater speed in identifying attacks and remedying them before they cause more damage. They also help meet regulation requirements that require security monitoring, vulnerability management, or an incident response function.

Recommended courses

SEC450 | SEC503 GCIA | SEC511 GMON | SEC555 GCDA | FOR508 GCFA | FOR572 GNFA | FOR532 | SEC504 GCIH

15 Security Awareness Officer (Security Awareness & Communications Manager)

Security Awareness Officers work alongside their security team to identify their organization's top human risks and the behaviors that manage those risks. They are then responsible for developing and managing a continous program to effectively train and communicate with the workforce to exhibit those secure behaviors. Highly mature programs not only impact workforce behavior but also create a strong security culture.

"This role allows me to use my previous experience to influence proper security behaviors, effectively improving our company's defenses. And the rapidly evolving nature of threats means my job is never boring."

- Sue DeRosier

Why is this role important?

People have become the top drivers of incidents and breaches today, and yet the problem is that most organizations still approach security from a purely technical perspective. Your role will be key in enabling your organization to bridge that gap and address the human side also. Arguably one of the most important and fastest growing fields in cyber security today.

Recommended courses

MGT433 SSAP | MGT512 GSLC | MGT521

16 Vulnerability Researcher & Exploit Developer (Vulnerability Assessment Analyst)

In this role, you will work to find 0-days (unknown vulnerabilities) in a wide range of applications and devices used by organizations and consumers. Find vulnerabilities before the adversaries!

"I think researchers will play a crucial role in years to come. They will be able to identify and help us prepare for the vulnerability before it is exploited by the hacker so instead of responding to incidents we will then be able to proactively prepare ourselves for the future issues."

- Anita Ali

Why is this role important?

Researchers are constantly finding vulnerabilities in popular products and applications ranging from Internet of Things (IoT) devices to commercial applications and network devices. Even medical devices such as insulin pumps and pacemakers are targets. If we don't have the expertise to research and find these types of vulnerabilities before the adversaries, the consequences can be grave.

Recommended courses

SEC660 GXPN | SEC661 | SEC670 | SEC760

17 Application Pen Tester (Secure Software Accessor)

Application penetration testers probe the security integrity of a company's applications and defenses by evaluating the attack surface of all in-scope vulnerable web-based services, client-side applications, servers-side processes, and more. Mimicking a malicious attacker, app pen testers work to bypass security barriers in order to gain access to sensitive information or enter a company's internal systems through techniques such as pivoting or lateral movement.

"It is not only about using existing tools and methods, you must be creative and understand the logic of the application and make guesses about the infrastructure."

- Dan-Mihai Negrea

Why is this role important?

Web applications are critical for conducting business operations, both internally and externally. These applications often use open source plugins which can put these apps at risk of a security breach.

Recommended courses

SEC542 GWAPT | SEC560 GPEN | SEC575 GMOB | SEC588 GCPN | SEC660 GXPN | SEC760

18 ICS/OT Security Assessment Consultant (ICS/SCADA Security Engineer)

One foot in the exciting world of offensive operations and the other foot in the critical process control environments essential to life. Discover system vulnerabilities and work with asset owners and operators to mitigate discoveries and prevent exploitation from adversaries.

"Working in this type of industry, I can see how the demand is increasing so rapidly that companies starting to desperately looking for people with proper skillsets."

- Ali Alhajhouj

Why is this role important?

Security incidents, both intentional and accidental in nature, that affect OT (primarily in ICS systems) can be considered to be high-impact but low-frequency (HILF); they don't happen often, but when they do the cost to the business can be considerable.

Recommended courses

ICS410 GICSP | ICS456 GCIP | ICS515 GRID | ICS612 | SEC560 GPEN

19 DevSecOps Engineer (Information Systems Security Developer)

As a DevSecOps engineer, you develop automated security capabilities leveraging best of breed tools and processes to inject security into the DevOps pipeline. This includes leadership in key DevSecOps areas such as vulnerability management, monitoring and logging, security operations, security testing, and application security.

"From my point of view it is a highly demanded position by companies which need to offer flexible, agile and secure solutions to their clients' developers."

- Antonio Esmoris

Why is this role important?

DevSecOps is a natural and necessary response to the bottleneck effect of older security models on the modern continuous delivery pipeline. The goal is to bridge traditional gaps between IT and security while ensuring fast, safe delivery of applications and business functionality.

Recommended courses

SEC488 GCLD | SEC510 GPCS | SEC522 GWEB | SEC540 GCSA

20 Media Exploitation Analyst (Cyber Crime Investigator)

This expert applies digital forensic skills to a plethora of media that encompasses an investigation. If investigating computer crime excites you, and you want to make a career of recovering file systems that have been hacked, damaged or used in a crime, this may be the path for you. In this position, you will assist in the forensic examinations of computers and media from a variety of sources, in view of developing forensically sound evidence.

"This is like solving a puzzle or investigating a crime. There is an exciting element to the unknown and the technical complexity of countermeasures. The sensitivity of content and potential to get real evidence on something is exciting."

- Chris Brown

Why is this role important?

You are often the first responder or the first to touch the evidence involved in a criminal act. Common cases involve terrorism, counter-intelligence, law enforcement and insider threat. You are the person relied upon to conduct media exploitation from acquisition to final report and are an integral part of the investigation.

Recommended courses

FOR308 | FOR498 GBFA | FOR500 GCFE | FOR508 GCFA | FOR518 GIME | FOR532 | FOR572 GNFA | FOR585 GASF