SANS | GIAC CERTIFICATIONS

NEW TO CYBER CAREER GUIDE 2024

NEW TO CYBER CAREER GUIDE

Table Of Contents

Introduction

Welcome to the world of cybersecurity, a dynamic and critical field dedicated to protecting digital assets and information from the ever-evolving spectrum of threats. This guide is designed for individuals who are new to cybersecurity, including recent graduates, career changers, and anyone curious about entering this vital industry. Our aim is to illuminate the pathways into cybersecurity, offer a glimpse into the daily life and responsibilities of various roles, and provide the necessary insights to help you navigate your budding career in this domain.

Cybersecurity is not a monolith; it encompasses a wide range of specialties, from the analytical rigor of Forensic Analysts and the strategic oversight of Security Managers to the technical acumen of Cloud Security Engineers and the investigative prowess of OSINT Investigators. Each role plays a crucial part in the cybersecurity ecosystem, safeguarding against data breaches, cyber-attacks, and other digital threats.

This guide draws from firsthand accounts and expert analyses to offer a comprehensive overview of what it's like to work in various cybersecurity roles. You'll find details on desired skills and experiences, work expectations and lifestyle, the positives and negatives of each role, and the types of backgrounds that can lead to a career in cybersecurity. Whether you're drawn to the analytical challenge of a SOC Analyst, the strategic depth of a Risk and Compliance Analyst, or the high-stakes environment of an Incident Response Handler, this guide serves as a starting point to explore where you fit in the cybersecurity landscape.

THE LIFE OF A

Security Operations Center (SOC) Analyst

SANS | GIAC CERTIFICATIONS

What Is a SOC Analyst?

SOC Analysts are the front-line defenders of an organization's cybersecurity posture. They are responsible for identifying and responding to security incidents, protecting against threats, and helping maintain a strong security posture to safeguard digital assets and sensitive information. The Security Operations Center (SOC) is the control center of an organization's IT assets that monitors, analyzes, and responds to potential security threats. They are mostly in large organizations, governments or third-party security companies that provide such services for many smaller organizations. While a SOC Analyst typically works in a Security Operations Center, many smaller organizations may have Security Analysts who perform similar security functions.

Desired Skills and Experience

What employers are typically looking for in their new hires.

- Needs to understand technical security issues
- Strong analytic and cognitive skills
- Attentive to detail and accuracy
- Those who can thrive in a fast paced environment

Work Expectations and Lifestyle

Life in the day of a SOC Analyst

A SOC Analyst may either play one specific role or may have multiple roles in their regular workflow. But generally, they monitor the current state of security of systems and networks in real time, analyze alerts and trends, and may generate or respond to alerts. SOC Analysts collaborate with incident response teams and other IT professionals to develop and execute incident response plans. They are using multiple tools and information feeds simultaneously to identify and respond to malicious activities. They communicate security issues to other teams such as Incident Response, Forensic Analysts and Threat Hunters.

While a SOC Analyst typically works set hours it's not always normal business hours as the

Types of Backgrounds

- Military
- Law Enforcement
- IT Help Desk
- Systems or Network Administrator
- Incident Response

THE LIFE OF A SECURITY OPERATIONS CENTER (SOC) ANALYST

SOC usually operates 24/7. They may be expected to work on holidays and weekends. The work is typically scheduled and consistent, but emergencies and long hours of shift work can occur. They are also typically involved in the incident response process, providing material support to other teams such as shutting down systems, disabling accounts, and facilitating communications.

Positives

The good fun things of the job

- Good work/life balance
- Good pay for entry level jobs
- Doesn't normally require a college degree or extensive education
- Exciting and dynamic work flows

Negatives

The not so fun things

- The job can be tedious with repetitive tasks.
- Must work well under pressure.
- Long hours of stress can contribute to job burnout.
- May be exposed to evidence of crimes, pornography, violence, etc.

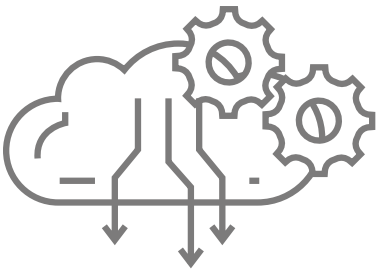
Types of backgrounds/Transferable Skills

- **Communication** | SOC analysts often need to communicate complex technical information to technical and non-technical audiences. They often write reports and narratives of an event after the event.
- **Teamwork** | SOC analysts are often part of a larger team so the ability to work effectively as part of a team is essential.
- **Adaptability** | The cyber landscape is constantly changing, so SOC Analysts need to be able to adapt to new threats and technologies quickly. Additionally, attacks and breaches can happen at any time, so SOC Analysts must be able to adapt to changing schedules and priorities.

THE LIFE OF A

SANS | GIAC CERTIFICATIONS

Cloud Security Engineer



What Is a Cloud Security Engineer?

A cloud security engineer works with systems administrators, network architects, and others to ensure that proper security objectives are met in the design, implementation, and maintenance of security measures to protect data, applications, and infrastructure hosted on cloud platforms. They play a crucial role in ensuring the protection of data and resources in cloud environments, while also mitigating the risks associated with cloud-based systems. The security engineer may need to tailor their efforts to a specific cloud environment (e.g., AWS, Azure, Google Cloud), integrate cloud-hosted resources with traditional data centers, or to have multiple cloud environments interact. They also ensure cloud environments comply with relevant regulatory requirements and industry standards (e.g., GDPR, HIPAA, PCI DSS).

Desired Skills and Experience

What employers are typically looking for in their new hires

- Familiarity with cloud computing platforms such as AWS, Azure, and/or Google Cloud
- Training in scripting and automation tools for security tasks (e.g., Python, PowerShell, Terraform).
- Excellent communication, teamwork and interpersonal skills to work collaboratively with colleagues and stakeholders
- Cloud certifications

Work Expectations and Lifestyle

Life in the day of a cloud security engineer

The daily tasks of a cloud security engineer can vary as well as be very specialized depending on the organization they are working for and the scope of the infrastructure they are managing. The general day-to-day workflow may include several different tasks including the configuration and deployment of security controls and solutions such as encryption, access controls, network security policies, to enhance the security posture of cloud environments. They collaborate with other members of the security team and relevant stakeholders to contain and mitigate security threats.

Types of Backgrounds

- Systems administration or network engineering
- Software development
- IT Security and compliance
- Data management and analytics
- Risk management, compliance and regulatory affairs
- Project management

The engineer typically identifies security tasks and workflows that can be automated using scripting languages or automation tools. They conduct audits and assessments to evaluate the effectiveness of security measures. Using the results of those assessments, the engineer provides security guidance to meet security and regulatory requirements and makes recommendations based on assessment findings for remediation. They also maintain and update documentation of security configurations, procedures, and incident response plans along with organizational security policies, standards, and guidelines as needed to reflect changes in cloud environments or security requirements.

✚ Positives

The good, fun things of the job

- Great job opportunities and career advancement prospects
- Challenging and rewarding work that is intellectually stimulating and rewarding
- Competitive compensation due to the high demand for cloud security expertise
- Opportunities for advancement
- Remote work opportunities

▬ Negatives

The not so fun things

- Complexity and technical depth of cloud environments can require advanced technical expertise and experience in some job roles
- High pressure and responsibility to secure cloud environments
- Continuous learning curve in keeping up with cloud platform changes
- Burnout and stress due to the high-pressure nature of the job

Transferable Skills

IT operations experience—Individuals with experience in IT operations or systems administration have a strong understanding of infrastructure components, networking, and system configurations essential for securing cloud environments effectively.

Software development skills—Software developers possess skills in programming languages, automation, and scripting, which are highly relevant to cloud security.

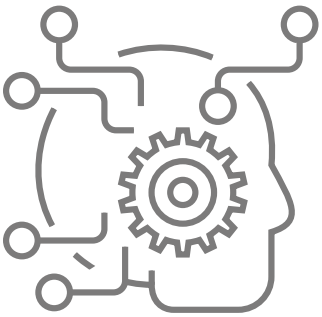
Networking expertise—Professionals with expertise in networking understand network protocols, routing, and firewall configurations, can apply this knowledge to design and implement secure network architectures in the cloud.

Compliance and risk management—Individuals with experience in compliance, risk management, or audit roles can apply this knowledge to ensure cloud environments meet regulatory standards and address security risks effectively.

Project management skills—Project managers bring skills in planning, organization, and coordination, which are valuable for managing cloud security projects and initiatives. They can oversee the implementation of security controls, track progress, and communicate effectively with stakeholders.

THE LIFE OF A

Incident Response Handler



What Is a Incident Response Handler?

An incident response handler's primary role is to minimize the impact of security breaches or incidents, such as data exfiltration, malware infections, or network intrusions. They are responsible for implementing a real-time defensive response to ongoing cybersecurity incidents. Handlers typically possess a strong understanding of cybersecurity principles, as well as technical skills in areas such as systems management, networking, malware analysis, digital forensics, and incident management tools. They must also be able to work effectively under pressure, prioritize tasks, and communicate complex technical information clearly to non-technical stakeholders.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Ability to aggregate and analyze information from multiple sources
- Adaptability to quickly learn and apply new technologies and techniques
- Attention to detail and the ability to document events accurately
- Strong problem-solving skills and the ability to think critically under pressure
- Strong organizational and time management skills to effectively prioritize tasks and manage multiple incidents simultaneously

Work Expectations and Lifestyle

Life in the day of a incident response handler

A day in the life of an incident response handler is dynamic and can involve a mix of proactive threat hunting, incident response activities, communication with multiple stakeholders, and continuous learning to stay ahead of evolving cybersecurity threats. Their daily activities will vary depending on the organization, the current threat landscape, and any ongoing security incidents. When a handler is not working on an active incident a typical routine at the start of their shift begins with a debrief from the previous shift, reviewing security monitoring systems and security information and event management (SIEM) tools for any unusual activity or potential security incidents that occurred during off-hours. They also actively monitor events of interest throughout the day, watching for alerts or incident tickets that may come in at any time.

Types of Backgrounds

- Law enforcement/intelligence analyst
- Military/defense specialist
- Security analyst
- Network or systems administrator
- IT support specialist
- Forensic analyst
- Penetration tester/ethical hacker
- Compliance auditor/analyst

During an active incident, the handler's activities change significantly as they coordinate with other members of the incident response team, including IT staff, security analysts, and management, to formulate a response plan. In concluding an incident, they conduct post-incident reviews and analysis to identify areas for improvement in incident detection, response, and mitigation. They also document their activities and observations throughout the day, then pass along time-sensitive information to the next shift as they conclude their day.

Positives

The good, fun things of the job

- Stimulating and challenging work
- Continuously evolving learning opportunities
- Impactful work to the organization and the community
- Interesting problem-solving challenges

Negatives

The not so fun things

- High stress levels due to high-stakes decision making
- Long work hours and on-call responsibilities can lead to work-life balance issues and burnout
- The complexity of incidents can be mentally exhausting
- Continuous pressure to perform can take an emotional toll

Transferable Skills

Attention to detail—Individuals with backgrounds in fields requiring meticulous attention to detail, such as accounting, quality assurance, or research, may excel in incident response roles.

Adaptability—People with backgrounds in dynamic environments, such as military service, emergency response, or project management, may possess strong adaptability skills that can be valuable in incident response.

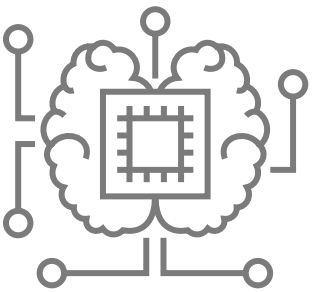
Teamwork and collaboration—Individuals with backgrounds in team-oriented environments, such as sports teams, volunteer organizations, or group projects, may have valuable teamwork and collaboration skills.

Leadership skills—Individuals with backgrounds in leadership positions, such as project management, supervisory roles, or community leadership, may have transferrable leadership skills that can be applied in incident response.

THE LIFE OF A

OSINT Investigator

SANS | GIAC CERTIFICATIONS



What Is a OSINT Investigator?

OSINT investigations may be conducted for various purposes including cybersecurity operations, law enforcement, corporate intelligence, due diligence, competitive analysis, and research. An OSINT (Open Source Intelligence) investigator specializes in gathering information from publicly available sources on the internet such as web pages, social media, news articles, public records, and other openly available sources. Investigators use various techniques and tools to collect, analyze, and interpret information to uncover insights, trends, patterns, or connections related to a particular subject, individual, organization, or event. Their goal is to take collected data and turn it into intelligence for a stated end goal.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Creative thinking, pattern matching, identifying trends and draw meaningful insights from disparate sources of information
- Demonstration of strong analytical and critical thinking skills
- Soft skills such as communication, teamwork, problem-solving, and leadership
- Adaptability and willingness to learn

Work Expectations and Lifestyle

Life in the day of a OSINT investigator

A typical day for an OSINT investigator can vary greatly depending on the work they are tasked with and where they are in the steps toward their goals. A significant portion of their day may be dedicated to conducting online research and analysis. Other time may be focused on gathering, analyzing, and interpreting information from various online sources to support investigations and decision-making processes. This could involve scouring various sources such as social media platforms, news websites, forums, public records databases, and other online sources to gather relevant information. Investigators typically document their findings, including relevant details, sources, timestamps, and any other pertinent information. This documentation is essential for creating reports, sharing findings with colleagues or clients, and maintaining an organized record of the investigation.

Types of Backgrounds

- Law Enforcement or military intelligence analyst
- Cybersecurity analyst
- Journalist or investigative teporter
- Digital forensic examiner
- Research analyst or market researcher
- Compliance officer or regulatory analyst

Positives

The good, fun things of the job

- Variety and diversity keeps the work interesting and dynamic.
- An investigator may have a degree of flexibility and autonomy in how they approach their work. This could include setting their own schedules, choosing investigative techniques, and managing their workflow.
- Many aspects of OSINT work can be conducted remotely, allowing investigators to work from virtually anywhere with an internet connection.

Negatives

The not so fun things

- The information overload of sorting through vast amounts of information from various sources can be overwhelming and time-consuming.
- Sorting through false information, misinformation, and disinformation can be challenging and may lead to incorrect conclusions if not properly vetted.
- The fast-paced nature of OSINT work, combined with the pressure to uncover timely and actionable intelligence, can lead to burnout. Long hours, tight deadlines, and the constant demand for results can take a toll on mental and emotional well-being.
- There can be an emotional toll with investigating sensitive or distressing topics. Topics such as criminal activities, human rights violations, or traumatic events can take an emotional toll on investigators. Exposure to disturbing content or engaging with victims of crime or conflict may lead to compassion fatigue or secondary trauma.

Transferable Skills

Research skills—Individuals with experience in academic research, journalism, market research, or investigative reporting often possess valuable skills in conducting thorough and systematic research.

Critical thinking—People with backgrounds in fields such as philosophy, logic, law, or academia may have honed their critical thinking abilities, which can be applied to analyzing complex data sets and drawing informed conclusions.

Analytical skills—Those with backgrounds in data analysis, statistics, mathematics, or computer science may have developed strong analytical skills that are highly applicable to OSINT work, particularly in tasks such as data mining, pattern recognition, and trend analysis.

Adaptability and problem-solving skills—Individuals with experience in dynamic and fast-paced environments, such as emergency services, military, or project management, may have developed strong problem-solving and adaptability skills that are valuable in OSINT work.

THE LIFE OF A

Forensic Analyst

SANS | GIAC CERTIFICATIONS

What Is a Forensic Analyst?

Forensic analysts are the investigators after the fact of a breach or incident. The analyst is a professional who investigates cybercrimes, security breaches, and digital incidents by analyzing digital evidence. Their primary responsibility is to gather, preserve, analyze, and present digital evidence in legal or administrative proceedings. Their job is to collect and analyze the evidence at hand to put attribution to the malicious actor's activities. They employ a variety of techniques and tools to uncover evidence of cyber-attacks, data breaches, hacking incidents, and other digital crimes.

While technical expertise is important, a forensics investigator also must be able to take large amounts of information and distill it into intelligence and reconstruct events based on the evidence available. A digital forensics analyst is responsible for investigating and analyzing digital evidence related to cybercrimes and other digital incidents. This role requires a diverse skill set to effectively navigate the complex world of digital data and uncover crucial information.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Needs to understand technical security issues
- Strong analytic and cognitive skills
- Able to apply scientific principles and objective thinking
- Attentive to detail and accuracy

Work Expectations and Lifestyle

Life in the day of a forensic analyst

A day in the life of a forensic analyst may be dynamic and varied, often involving a mix of technical analysis, documentation, collaboration, and legal or administrative tasks as they work to uncover digital evidence and support investigations into cybercrimes and security incidents. Depending on the nature of their current cases, a forensic analyst may spend part of their day collecting digital evidence from various sources. This could involve taking custody of computers, mobile devices, or other electronic equipment for forensic examination, or remotely accessing network logs and other digital artifacts. They must ensure the integrity and preservation of digital evidence through proper handling and documentation to maintain its admissibility in legal proceedings.

Types of Backgrounds

- Military cyber operations or law enforcement
- Intelligence operatives
- Legal professionals
- Data analyst or data scientist

The analyst may participate in incident response activities to contain and mitigate the impact of cyber incidents, while also collecting evidence for further analysis. They document findings and prepare reports that summarize the analysis, findings, and conclusions for use in legal proceedings or organizational decision-making. They may also provide expert testimony and support to law enforcement agencies, legal teams, and other stakeholders during legal proceedings.

Positives

The good, fun things of the job

- Stimulating work using problem solving skills
- Make a difference by exposing the actions of bad actors
- Fulfilling work making a positive impact
- High demand due to increasing frequency and sophistication of cybercrimes
- Flexible Work Environment

Negatives

The not so fun things

- Emotional stress of possible encounters with disturbing or distressing content: evidence of crimes, pornography, violence, etc.
- High-stakes work and responsibility to ensure that evidence is collected, analyzed, and preserved accurately, as any mishandling could have serious consequences.
- Repetitive tasks, such as data collection, documentation, and analysis, can lead to boredom or job dissatisfaction over time.
- The workload of a cyber forensic analyst can vary greatly depending on the volume and severity of cyber incidents. Periods of intense activity may be followed by lulls, leading to unpredictable work schedules.

Transferable Skills

Analytical skills—Individuals with backgrounds in fields such as data analysis, mathematics, or research often possess strong analytical skills that can be applied to digital forensic investigations.

Problem-solving skills—Previous experience in roles that involve troubleshooting technical issues or devising solutions to complex problems can be highly beneficial.

Attention to detail—Individuals with backgrounds in roles that demand attention to detail, such as quality assurance, accounting, or regulatory compliance, can excel in cyber forensics.

Technical proficiency—While a background in cybersecurity or IT is advantageous, individuals with technical aptitude and a willingness to learn can also succeed in cyber forensics.

Communication skills—Effective communication skills are essential for cyber forensic analysts to convey their findings, write comprehensive reports, and provide expert testimony in legal proceedings.

Ethical integrity—Previous experience in roles that prioritize ethical conduct, such as law enforcement, healthcare, or legal professions, can instill the values necessary for success in cyber forensics.

THE LIFE OF A

SANS | GIAC CERTIFICATIONS

Risk and Compliance Analyst

What Is a Risk and Compliance Analyst?

A risk and compliance analyst is tasked with the organizationally important job of determining whether the organization is meeting their security objectives. The analyst's job is to determine that the stated objectives are recorded, meet all compliance requirements and security best practices, and they are meeting those stated objectives. Along with documenting the current security state and changes over time, the analyst works with others to plan and meet future security and compliance objectives.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Must have good planning and project management skills
- Strong communication skills both in writing as well as verbal skills
- Needs to understand the role policy, compliance and the law play in meeting the security objectives of the organization
- Must possess general knowledge of the technologies used in the security of the organization
- Ability to think and reason in the abstract as well as application of specific technologies

Work Expectations and Lifestyle

Life in the day of a risk and compliance analyst

The main role of a risk and compliance analyst is to be a documenter and intermediary focused on the security objectives of an organization. An analyst spends much of their day in meetings, writing and reading reports and other documentation. They speak with both the non-technical and technical people in the organization as well as external vendors and service providers. They are communicators, collecting information, processing it, and then sharing it with technical and non-technical decision makers. They are also involved in recording the decisions made to codify into policy and procedure.

Types of Backgrounds

- Project management
- IT help desk
- Communications
- Psychology
- Compliance

The work schedule of an analyst is typically the normal working hours of the organization and are rarely needed to work odd hours or respond to emergencies. The analyst typically works normal business hours and on rare occasions are needed to work overtime. The scheduled nature of the work means that there is usually flexibility in life activities such as personal appointments and family commitments. Work from home can be an option offered by employers as much of the work the analyst performs may not need to be in person.

✚ Positives

The good, fun things of the job

- Excellent work/life balance
- Typically in a low-stress environment
- Doesn't require extensive technical skills
- Meet and talk to many people in different roles
- May have flexible schedule
- Remote work possible

▬ Negatives

The not so fun things

- The job can be tedious with repetitive tasks
- Must manage workflows and projects
- Recommendations can go unheeded

Transferable Skills

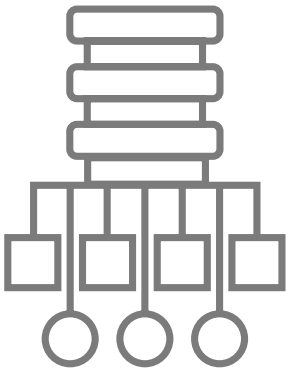
Communication—Those strong in the soft skills of communication, logical thinking, and attention to detail, can be trained on the technologies while on the job. They must communicate with technical and non-technical audiences.

Teamwork—The analyst works with other teams so the ability to work effectively as part of a team is essential.

Project management and planning—While a risk and compliance analyst doesn't necessarily need intimate knowledge of, or hands-on experience with, security hardware and software they will need to know generally what the technologies are and what they are used for.

THE LIFE OF A

Cybersecurity Auditor



What Is a Cybersecurity Auditor?

A cybersecurity auditor is responsible for evaluating and assessing an organization's information systems, networks, and infrastructure to ensure they comply with established security policies, standards, and regulations. Their primary objective is to identify vulnerabilities, weaknesses, and potential risks that could compromise the confidentiality, integrity, and availability of data and systems. Overall, cybersecurity auditors play a crucial role in helping organizations assess and improve their security posture, mitigate risks, and ensure compliance with applicable regulations and standards.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Audit and compliance knowledge
- Risk assessment skills
- Communication and people skills
- Great attention to detail
- Ethical standards

Types of Backgrounds

- IT support specialist
- Systems or network administrator
- Software developer
- Penetration tester/ethical hacker
- Compliance officer/security analyst/SOC analyst

Work Expectations and Lifestyle

Life in the day of a cybersecurity auditor

The professional life of a cybersecurity auditor is multifaceted, involving a combination of technical analysis, communication, collaboration, and continuous learning to help organizations effectively manage cybersecurity risks and ensure compliance with relevant standards and regulations. They review and analyze the organization's security policies, procedures, and guidelines to ensure they align with best practices and regulatory requirements. They conduct meetings with stakeholders and technical people.

The auditor may spend a significant portion of their time planning and preparing for upcoming audits or assessments. This could involve reviewing audit objectives, scope, and documentation, as well as coordinating with other team members or stakeholders involved in the audit process. They conduct risk assessments, identifying and evaluating potential security risks and threats to the organization's IT assets. They also audit systems for compliance with relevant laws, regulations, and industry standards related to cybersecurity, such as GDPR, HIPAA, PCI DSS, ISO 27001, etc. After gathering evidence and completing audit activities, the auditor may spend time documenting findings, observations, and recommendations in audit reports or other deliverables. This would likely involve writing detailed narratives, summarizing key findings, and compiling supporting evidence.

✚ Positives

The good, fun things of the job

- Impactful and meaningful work for the organization
- Good work-life balance in terms of work location and schedule
- Possible remote work opportunities

▬ Negatives

The not so fun things

- High pressure to balance the needs of the organization with security
- There may be many repetitive tasks
- The field of cybersecurity is highly technical and constantly evolving, requiring security auditors to stay updated with the latest technologies, threats, and best practices
- Navigating complex regulatory landscapes with multiple frameworks can be time-consuming and challenging

Transferable Skills

Analytical skills and problem-solving abilities—Individuals with backgrounds in fields such as engineering, mathematics, or data analysis often possess strong analytical skills, which are valuable for identifying patterns, trends, and anomalies in security data and audit findings.

Project management experience—Professionals with experience managing projects or leading teams can bring valuable organizational, time management, and communication skills to the role of a security auditor, helping to prioritize tasks, meet deadlines, and coordinate audit activities effectively.

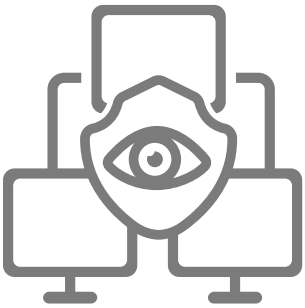
Risk management knowledge—Experience in risk management, financial analysis, or insurance underwriting can provide a solid foundation for understanding risk assessment methodologies and frameworks, which are central to the work of a security auditor.

Technical proficiency—While not always necessary, individuals with technical backgrounds in fields such as computer science, information technology, or cybersecurity may have a head start in understanding technical aspects of security auditing, such as network protocols, system configurations, and cybersecurity tools.

THE LIFE OF A

SANS | GIAC CERTIFICATIONS

Cybersecurity Manager



What Is a Cybersecurity Manager?

A cybersecurity manager plays a critical role in safeguarding an organization's digital assets and maintaining the confidentiality, integrity, and availability of its information systems. The manager is responsible for overseeing an organization's (or department's) cybersecurity strategy and implementation of security measures to protect the organization's digital assets, systems, and data from cyber threats. Their role involves identifying potential vulnerabilities, assessing risks, developing, and implementing security protocols, monitoring for security breaches, and responding to incidents. Their responsibilities may include developing and implementing cybersecurity policies and procedures along with conducting risk assessments and vulnerability scans to identify potential threats. They manage the security team and the supporting security infrastructure.

Desired Skills and Experience

What employers are typically looking for in their new hires

- Understand and manage a security budget
- Strong communication and people skills
- Analytical and problem-solving skills
- Adaptability and willingness to learn
- Teamwork and collaboration skills

Work Expectations and Lifestyle

Life in the day of a cybersecurity manager

The role of a cybersecurity manager involves a combination of strategic planning, operational oversight, team management, and continuous learning to effectively protect an organization's digital assets and mitigate cyber risks. They collaborate with other departments, such as IT, legal, and compliance, to ensure alignment with organizational goals and regulatory requirements along with developing incident response plans and leading response efforts during security incidents. They must keep up to date with the latest cybersecurity threats, trends, and technologies to continually improve security measures.

Types of Backgrounds

- Security analyst or engineer
- System administrator or network administrator
- Compliance officer or auditor
- Risk analyst or risk manager
- Project manager
- Law enforcement or military

The cybersecurity manager meets with other management or stakeholders, regulatory authorities, auditors, or compliance teams to discuss cybersecurity strategy, upcoming projects, or policy updates. They work on developing or updating cybersecurity policies, procedures, and guidelines to address evolving threats and regulatory requirements. They communicate with external vendors or partners to assess their security posture, review contracts or agreements, and ensure compliance with security requirements.

Positives

The good, fun things of the job

- Challenging and rewarding work
- Perform an impactful role in protecting organizations from cyber threats
- Variety of interesting responsibilities
- Opportunities for advancement into higher-level roles such as chief information security officer (CISO), security consultant, or executive leadership positions

Negatives

The not so fun things

- Cybersecurity managers often lead in high-stress situations
- Rapidly evolving nature of cybersecurity creates a constant learning curve
- Skills shortage and talent gap in hiring new security team members
- Demanding nature of cybersecurity roles can negatively impact work-life balance
- Burnout risk due to the high-stress levels, long hours, and constant pressure

Transferable Skills

Analytical skills—Professionals with backgrounds in fields such as engineering, mathematics, or data analysis often possess strong analytical abilities.

Problem-solving skills and attention to detail—These abilities are essential in cybersecurity management for identifying security vulnerabilities, troubleshooting technical issues, and developing effective solutions to mitigate risks.

Project management and communication skills—Effective planning and communication skills are crucial for cybersecurity managers, including project vision and planning, organization, and resource management skills are desirable.

Leadership and team management skills—Managers must demonstrate strong leadership skills, such as delegation, motivation, trust, and accountability.

Conclusion

Having delved into the lives of those at the heart of cybersecurity, you now have a window into the diversity of roles, responsibilities, and opportunities that define this field. The journey into cybersecurity is as varied as the individuals who populate it, with multiple pathways leading to rewarding careers.

Key Takeaways:

- Diverse Opportunities: Cybersecurity offers a broad spectrum of roles, each with its unique challenges and rewards. Whether your strengths lie in technical, analytical, managerial, or investigative skills, there is a niche for you.
- Continuous Learning: The dynamic nature of cyber threats necessitates ongoing education and adaptation. Embrace the opportunity for continuous learning and professional development to stay ahead in the field.
- Practical Experience: Hands-on experience, whether through internships, certifications, or personal projects, is invaluable. Engage actively with the community and seek out practical opportunities to apply your growing knowledge
- Networking: Building a professional network with the cybersecurity community can provide support, mentorship, and opportunities. Attend conferences, participate in forums, and connect with peers and experts.

What to Do Next:

1. Assess Your Interests and Skills: Reflect on what aspects of cybersecurity excite you and where your strengths lie. Use this guide to identify roles that align with your interests and abilities.
2. Seek Education and Training: Consider pursuing relevant education, certifications, and training programs to build the foundational knowledge and skills required for your chosen role.
3. Gain Practical Experience: Look for internships, volunteer opportunities, or projects that offer hands-on experience. Engaging with real-world challenges will enhance your understanding and appeal to potential employers.
4. Network and Connect: Join cybersecurity communities, attend workshops and conferences, and reach out to professionals in your area of interest. Networking can open doors and provide valuable insights into your career journey.

Embarking on a career in cybersecurity is a commitment to lifelong learning and adaptation. As you navigate this path, remember that your unique perspective and skills can make a significant impact on the safety and security of digital environments. The need for dedicated, skilled professionals has never been greater, and your journey into cybersecurity is not just a personal achievement but a vital contribution to the security of our world.

Resources

To learn about other careers in the cybersecurity field, check out the **20 Coolest Careers in Cybersecurity** poster

SANS New2Cyber Summit 2023: Reskilling Edition Videos

SANS New2Cyber Summit 2022 Videos

Reach the peak of your cyber security career with **SANS Summits**

SANS Cyber Academies