Cyber Security HIGHGATE

WHITE PAPER

Top 14 Steps to Hire a Top-Notch Security Analyst or Security Program Manager

September 5, 2023

www.highgatecybersecurity.com

Contents

Introduction

In today's rapidly evolving digital landscape, the threat of cyber-attacks has escalated at an alarming rate, making the demand for skilled information security practitioners more critical than ever. The surge in cybercrime coincides with a global shift towards cloud and hybrid/multi-cloud storage and processing, increased digitization across various sectors, such as healthcare and utilities, and the remote administration and management of IT environments. As a result, the need for cybersecurity expertise is not only growing, but it is evolving to meet the challenges of a new digital era. According to the US Bureau of Labor Statistics, employment of information security analysts is projected to grow by 35% from 2021 to 2031, a rate much faster than the average for all occupations. This translates to an average of 19,500 job openings for information security analysts annually over the decade.

Objectives

The primary goals of this paper are to provide insightful suggestions and strategic approaches for human resources professionals tasked with hiring top-notch security analysts or security program managers. Although we have tailored our recommendations to the banking sector, the strategies outlined here apply to virtually any business needing to bolster its cybersecurity team. Every step requires a meticulously thought-out and strategic approach, from the initial search to the interview process and ultimately positioning the opportunity to the candidate.

Tactics in Research

Hiring the right individuals for critical positions, such as security analyst or security program manager, is crucial for safeguarding an organization's sensitive information. In this section, we outline steps designed to guide you in identifying and recruiting the most qualified candidates for these pivotal roles.

1. **Define Clear Job Requirements:** Begin by delineating the roles and responsibilities of the positions. Determine the skills, qualifications, and experience necessary for the security analyst and program manager roles. Collaborate with your organization's security team to pinpoint the critical competencies required.
2. **Craft a Compelling and Specific Job Description:** Compose a detailed and enticing job description emphasizing the responsibilities, qualifications, and opportunities for growth associated with the roles. Be explicit about the nature of the security projects the candidates will manage.
3. **Leverage Professional Networks:** Use your professional network and connections within the cybersecurity industry to obtain referrals. Often, top candidates are discovered through word-of-mouth recommendations.
4. **Use Online Job Portals:** Advertise the job vacancies on pertinent job portals and professional networking platforms. Sites like LinkedIn, Indeed, ZipRecruiter, and specialized cybersecurity job boards like CyberSecurityJobs can help attract qualified candidates.
    - CyberSecurity Ventures Job Boards
    - InfoSec Jobs](https://infosec-jobs.com/
    - Careers in Cyber
    - Ninja Jobs
5. **Participate in Cybersecurity Events:** Engage in industry-specific events, conferences, and meetups related to cybersecurity. These functions provide opportunities to network and interact with potential candidates. Here are some examples:
    - Black Hat
    - RSAC
    - ISC Congress
    - InfoSec World
6. **Utilize Social Media:** Harness the power of social media platforms to publicize job openings and reach a broader audience. Engage with cybersecurity communities and groups to spread the word.

7. **Screen Resumes Thoroughly:** Scrutinize candidates' resumes and cover letters meticulously. Seek out relevant experience, appropriate certifications (examples provided below), and a genuine enthusiasm for cybersecurity. This field presents formidable challenges; therefore, individuals who are motivated by these challenges will possess a diverse array of experiences and demonstrate a keen interest in safeguarding vital assets. Remember, a candidate's resume is often their first opportunity to make a strong impression. Hence, a well-constructed resume that highlights relevant skills, certifications, and a passion for the field can be a strong indicator of a candidate's suitability for the role.

Certification	LinkedIn	Indeed	Simply Hired	Total
CISSP	159,912	14,401	8,780	183,093
CISA	37,606	7,688	4,019	49,313
Security+	7,366	10,161	3,235	20,762
CEH	16,402	2,425	1,468	20,295
CISM	8,436	4,145	2,573	15,154
GSEC	4,335	3,062	2,308	9,705
SSCP	4,046	3,013	2,160	11,865
CASP	3,783	1,128	868	5,778
GCIH	3,166	2,010	1,403	6,569
OSCP	2,095	1,850	946	4,891

Figure 1: Number of US job search results for certifications as of December 2022

Conduct Thorough Interviews: Prepare a comprehensive interview process that includes behavioral, technical, and situational questions. Involve your organization's security team in the interview process to evaluate technical skills and cultural fit.

Situational Question Examples

Below are some examples of situational questions.

- Can you share an instance where you had to troubleshoot a problem with a security system or program?
- How would you respond to unusual activity observed on a company's security systems?
- Can you recall a situation where you had to work with compliance laws and regulations? What challenges did you face, and how did you overcome them?
- Describe a situation where your employer needed to enhance data security. What strategies did you recommend? What challenges did you encounter, and how did you address them?
- Can you provide an example of a time when you had to perform a risk assessment? What process did you follow? Who else was involved? How did you address the issues?

Here are examples of technical skills for a cybersecurity analyst:

1. **Scripting:** Proficiency in building tools and automating repetitive tasks using scripting[1] Languages like Python or PowerShell enhance an analyst's productivity.
2. **Controls and Frameworks:** A cybersecurity framework encompasses best practices, policies, tools, and security protocols designed to secure an organization's data and operations. Example frameworks include:
    - NIST Cybersecurity Framework
    - ISO 27001 and ISO 27002
    - SOC2
    - NERC-CIP
    - HIPAA
    - GDPR
    - FISMA

The NIST CSF is a prevalent example. Control is a measure a company implements to protect against vulnerabilities and attacks. Common cybersecurity frameworks include:

- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- Center for Information Security (CIS)

[1] Scripting is a type of coding in which you make a program do something. The difference is that coding is static, whereas scripts can make images and text move around.

- System and Organization Controls 2 (SOC 2)

3. **Intrusion Detection:** Cybersecurity analysts must monitor network activity for potential intrusions. Proficiency in using intrusion detection software—SIEM products, IDS, and IPS—is essential for identifying suspicious activity or security violations.
4. **Network Security Control:** A comprehensive understanding of wired and wireless networks and how to secure them is crucial, as many cyberattacks occur across a network of connected devices.
5. **Operating Systems:** Competent security analysts are familiar with operating systems such as MacOS, Windows, Linux and their command-line interfaces. Many also understand the threats and vulnerabilities associated with mobile operating systems like iOS and Android.
6. **DevOps:** Organizations are increasingly focusing on security in software development and operations (DevOps) to reduce the risks of breaches caused by insecure applications.
7. **Regulatory Guidelines:** Does the analyst have knowledge of relevant regulatory and compliance frameworks? For example, PCI-DSS in finance, HIPAA in healthcare, GDPR for global privacy, or NERC CIP for electric power plants. Cybersecurity analysts help protect the organization from attack, theft, and loss while ensuring compliance with industry regulations.
8. **Offer Competitive Compensation:** To attract top talent, offer competitive salary packages and benefits that align with industry standards.

Assessing Qualities in the Candidate

9. **Assess Problem-Solving Abilities:** Incorporate practical exercises or problem-solving scenarios during the interview process to evaluate the candidate's ability to tackle real-world security challenges. For example, you can ask candidates how they would respond to a hypothetical security breach.
10. **Evaluate Soft Skills:** A security analyst or program manager requires excellent communication, teamwork, and leadership skills. Assess these soft skills during the interview process. Request examples of presentations or updates that the candidate has produced.
11. **Check References:** Confirm the candidates' qualifications and work history by checking references from previous employers or colleagues. We recommend asking probing questions such as:
    - Did the candidate ever respond to a security breach? How did they respond, and what did they do well?

- Can you provide examples where the candidate worked in a team environment? How did they perform in terms of collaboration, communication, and teamwork?
- How does the candidate behave under pressure?
- How passionate is the candidate about cybersecurity? Do they have the drive to continually learn about new technologies and threats and help protect the organization?

12. **Look for Passion and Continuous Learning:** Target candidates who are passionate about cybersecurity and demonstrate a commitment to continuous learning. Cybersecurity is a rapidly evolving field, and the best professionals stay abreast of the latest trends and threats.

Presenting the Opportunity to the Candidate

13. **Emphasize the organization's Commitment to Security:** Highlight the Organization's dedication to cybersecurity and the resources available to support the security team. Demonstrating the organization's commitment to protecting its assets and customers can attract top candidates.
14. **Promote Career Advancement Opportunities:** Highlight the potential for career growth and advancement within the organization's cybersecurity department. Top professionals often seek opportunities for more significant responsibilities and leadership roles.

Conclusion

Recruiting top-notch cybersecurity analysts and security program managers can be a challenging task. However, by being proactive and focused, you can increase your chances of hiring exceptional candidates who will contribute to your organization's cybersecurity success. With the ever-increasing demand for cybersecurity professionals, it's vital to have a thorough recruitment process that accurately identifies the best candidates. By following the steps mentioned above, you can ensure that you are hiring the right people for the job and keeping your organization's data safe and secure.

Protect your enterprise and your reputation

Highgate's mission is to help protect organizations and their reputations against cyber security threats by using the best people, solutions, and services possible.

Highgate's vCISO program and its vCISOs have collectively served hundreds of customers with a desire to drive value for the client and protect their organizations using a substantial set of proven services and people who have decades of real-world cyber security experience. 75% of Highgate vCISOs have between 10 and 20 years of cybersecurity experience and possess degrees and certifications (e.g., CISM, CISSP).

HIghgate's alliances mean our team stays connected to some of the latest developments in the cybersecurity/IT, AI, and cloud arena; alliances include AWS, IBM, and KnowBe4.

Highgate Cyber Security is headquartered in Austin, Texas, and operates out of several states in the USA, including Santa Clara, CA, Reno NV, Minneapolis MN, Chicago IL, and the United Kingdom.

Learn more at www.Highgatecybersecurity.com or contact us at BD@Highgatecybersecurity.com.