

The SOC hiring handbook

Your guide to building and retaining a strong security team



TABLE OF CONTENTS

| | |
|---|-----------|
| The SOC hiring handbook | 3 |
| Introduction | 3 |
| Hiring challenges | 4 |
| Finding top talent | 4 |
| Frequent turnover | 5 |
| Creating your hiring strategy | 6 |
| Justifying your hiring budget | 8 |
| Security operations organisational chart | 9 |
| Types of staffing models | 10 |
| Fully in-house | 11 |
| Fully outsourced | 12 |
| Hybrid | 13 |
| Building your SOC team | 15 |
| Chief Information Security Officer (CISO) | 16 |
| SOC Manager/Director | 17 |
| Security Engineer | 18 |
| Incident Responder | 19 |
| Security Analyst | 20 |
| Retaining your security team | 21 |
| Hire the right people | 23 |
| Advice from your peers | 24 |
| Optimise your job listings | 25 |
| Next steps | 26 |
| About LogRhythm | 27 |

The SOC hiring handbook

Introduction

A security operations centre (SOC) is like a machine. But like a machine, when one component is not working, performance can come to a standstill. Among the various elements—people, process, and technology—that are required to run an effective security operation, people are arguably the most important.

People are at the core of what makes a security operation a functional and scalable program, but in a market where security professionals are in high demand and there is little supply, it is a challenge to find and keep top talent.

A documented hiring strategy that addresses the goals of your security operation, chosen staffing model, required positions, and budget will help you build an effective team and identify gaps in your team. But where do you start? While there is no one-size-fits-all approach, you can use this handbook as a guide to create a strategy to find, hire, and retain top talent for your security operation regardless of your staffing model.

In this white paper, you will learn:

The challenges of building a security team and how to address them

- Why a hiring strategy is important to combat staffing challenges and building an effective security team
- How to plan for your staff while considering staffing models, budget, and organisation goals
- What key roles you need on your team and how to find and retain top talent

Hiring challenges

Whether you're building a team from scratch or you are responsible for adding staff to your current team, there are many challenges that can make finding, hiring, and retaining skilled security team members difficult.

In a time when catastrophic data breaches are on the rise, staffing a team that is prepared, passionate, and skilled is essential to protecting your organisation.



Finding top talent

We all know that there is a shortage of available security talent on the market. The high demand for skilled cybersecurity professionals is only increasing as the attack surface continues to grow and threat actors evolve at a rapid pace.¹

By 2022, the amount of unfilled cybersecurity positions is projected to reach 1.8 million², and the cybersecurity unemployment rate has dropped to zero per cent.³ Unfortunately, undergraduate and graduate education programs are not structured to give students the fundamental knowledge they need for a career in cybersecurity, and little is being done to increase awareness around cybersecurity as a career choice for students.⁴

¹ [The Cost of Cybercrime](#), Accenture, March 6, 2019

² [2017 Global Information Security Workforce Study](#), Frost & Sullivan

³ [Cybersecurity Unemployment Rate Drops to Zero Percent](#), Cybercrime Magazine, March 4, 2019

⁴ [Behind the Numbers on Why Universities Lag Behind in Cybersecurity Education](#), CloudPassage, April 13, 2016

Frequent turnover

Once you've made it past the challenge of finding people for your team, you will need to have a strategy in place to retain them. The endless amount of available security jobs makes turnover a common issue among security operations teams. In more cases than not, your team can easily find an opportunity for a higher salary if they decide to move on. Even if they are not looking for a new position, it's likely that they are being actively recruited if they have a strong skillset.

Employee turnover can unbalance workloads, put a damper on moral, and prohibit your team from maturing. According to a new ISACA report, 55 per cent of organisations say it takes them at least three months to fill open positions.⁵ Depending on the size of your security operations, a three-month period without a fully staffed team could put your organisation at a higher risk for attacks.



Recruiting talent with the essential skillsets needed to staff your security operation will continue to be one of the top challenges to building your team.

To minimise disruption and adequately protect your organisation while you work to backfill a position, your team should have systems in place to document processes and make knowledge easy to access and transfer.

Turnover is an inevitable part of a security team. A hiring strategy that includes a plan for how processes are documented and transferred to other team members will better equip you and your team to handle the challenges that turnover presents.

⁵ [State of Cybersecurity 2019](#), ISACA, 2019

Creating your hiring strategy

A documented hiring model for a SOC that includes clearly defined roles and responsibilities will make it easier for you to build a team from scratch or grow one that already exists.

Hiring strategies provide a blueprint for the people part of the business plan for your SOC, that will also include strategies for your processes and technologies. To create an effective hiring strategy, you must consider the goal of your security operations, your organisation's objectives, budget, and the staffing model that best suits your needs.

To combat the skills shortage and grow your team, you need to have a strategy in place that will help you identify the key roles you need to fill, as well as the most efficient and effective ways to fill those gaps.

There is not a one-size-fits-all approach.



Your hiring strategy should include a plan for retention and turnover to help prepare your team to handle both quickly. This should include a strategy for onboarding new hires and what a successful first 30, 60, and 90 days on the job would look like for your various team members. Setting expectations for your staff is just as important as the ROI you expect to see from your security technologies. It will require continuous check-ins, evaluations, and effective communication to set a staff member up for success in their new role.

Documenting your staffing strategy will help you to identify where you have gaps and areas for growth and improvement. When starting to create a strategy, you will need to make sure you have a plan for all elements of your security operations program, such as monitoring, detection, response, and recovery — whether these are handled in-house, outsourced, or via a hybrid model.

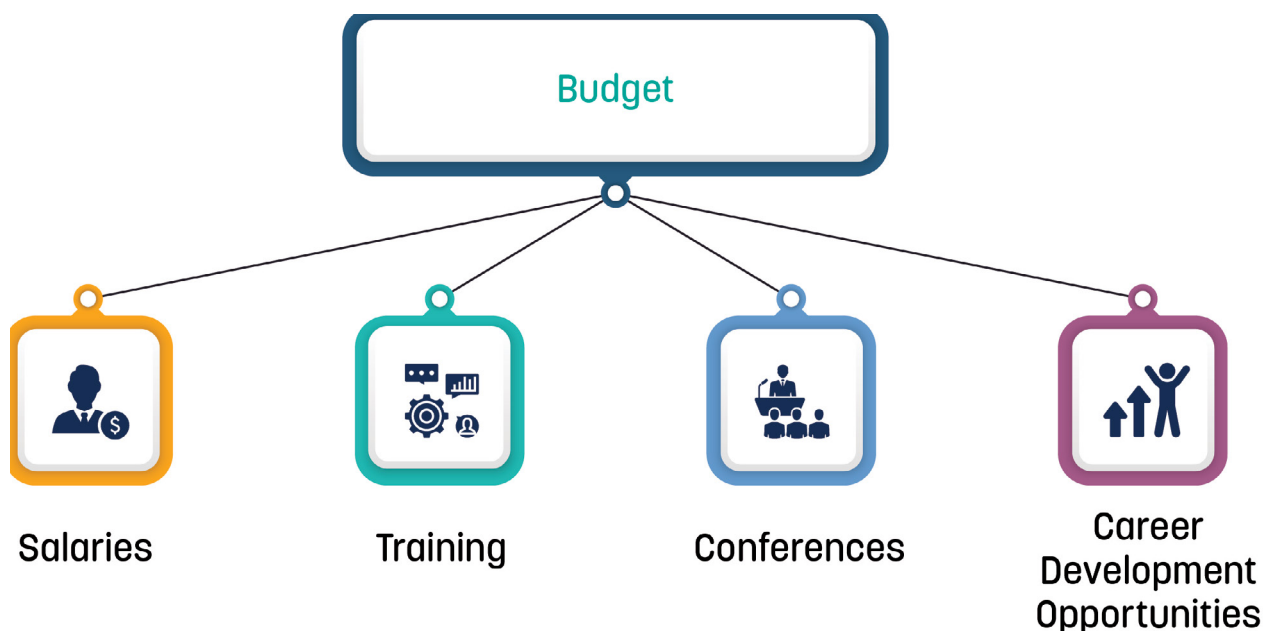
For most organisations, the SOC Manager oversees hiring for his or her team, because he or she manages the team and is responsible for their growth, development, and largely for their job satisfaction. The Chief Information Security Officer (CISO) / Chief Security Officer (CSO) / Chief Information Officer (CIO) should communicate their hiring strategy and budget with their SOC Manager so he or she can adequately make hires that align with the organisation's goals.

Without a hiring strategy, it will be challenging for a SOC Manager to prioritise and hire the right people. For these reasons, it will be imperative that your hiring strategy be well-documented, clear and executable.

Justifying your hiring budget

Once you determine the positions you need, the next step is to budget for your team. You will need to convince an executive team and board that you require a budget for your people that is adequate to manage your organisation's security risk. Part of reducing the risk of a breach is having essential roles and highly skilled people as part of your security operations, whether they are in-house or part of an MSSP.

In addition to attractive salaries, you will need to budget for training, conferences, and career development opportunities that are important variables candidates consider when they decide to join a team. Before you ask for your budget, you will need to have a plan in place that determines how you will allocate your budget across the roles you need to build your team. This includes getting creative with budget allocation. Think about the other departments your team could or does aid. Those teams may be willing to help fund certain resources for your SOC.



Security operations organisational chart

A well-defined organisational chart can help you to identify crucial roles and gaps on your team. The organisational chart can serve as a guide to the reporting structure and opportunities within your security operation and should be visible to your team. Share all or part of your hiring strategy and organisational chart during interviews to show candidates where security lies as a priority within the organisation.

The structure of a security operations centre can vary widely. Many of the differences are primarily related to the executive roles in a medium-to-large operation that might not exist within a smaller shop. Make sure to review and revise your organisational chart to reflect any changes that can occur as your company scales.

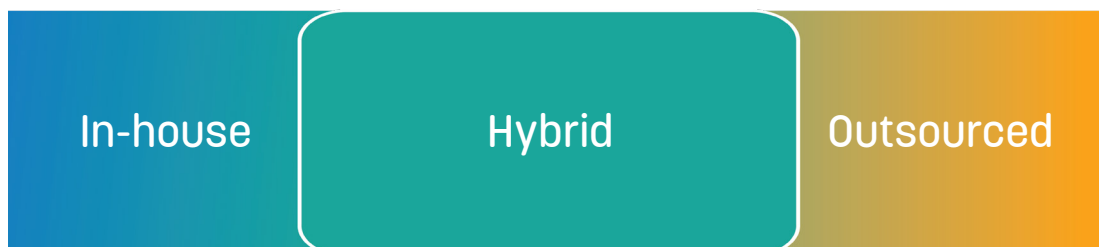
Types of staffing models

Whether you are building a security team from scratch or growing your current one, your hiring strategy will need to include a staffing model that fits your organisation's current and future objectives.

While there is no one-size-fits-all approach for every team, there are elements that will help you choose the best model for your operation, including:

- Your budget
- The size of your organisation
- The level of risk in your industry
- The level of risk your organisation is comfortable with
- The industry and the requirements for doing business in that industry for both your organisation and your customers
- The types of attacks that target your industry
- The amount of data your operation will handle on a day-to-day basis
- How quickly you need to build or grow your team

Following are definitions and conditions for common staffing models.



Fully in-house

A fully in-house staffing model requires you to fill all required positions for your security team internally.

Risk tolerance



If your organisation has a high tolerance for risk, then you may be able to achieve adequate protection with a small 8x5 team that is supplemented with automated escalations and notifications to your staff based on criticality and impact of any alert. If you're building a security team for a large organisation with a lower risk tolerance, than a fully in-house model would require you to have 24x7 team coverage.

Budget



Staffing a SOC entirely in-house requires a significant investment and the infrastructure to support your team. This model is typically best for larger organisations that have the budget and facilities to hire a team of essential and specialised staff.

Time



It can take considerable amounts of time to hire and onboard a fully in-house team. You should consider the level of risk your organisation will be under while you build your team and if you will be able to adequately protect your organisation while you find and hire staff. If your organisation is at a high risk for attack and has a low risk tolerance, then building a team from scratch in-house may not be the best staffing model for your hiring strategy (or you may need to consider an interim solution while you are onboarding).

Fully outsourced

In this model, you would rely on a managed security service provider (MSSP) to fill all of the roles of your security operations team.

Risk tolerance



Choosing whether your team could benefit from outsourcing versus keeping all your people and systems in-house requires an honest assessment of whether you will be able to protect your organisation for the level of risks it tolerates. You will also need to consider how imperative knowledge of your organisation or industry is to detect and prevent against potential threats. A fully outsourced option is great for organisations that have a low risk tolerance and do not require specialised knowledge related to the organisation or its industry.

Budget



The decision to hire an outside party to manage security should depend greatly on whether your resources are able to adequately detect, respond, and recover from a security event within your existing budget.

If the answer is no, then choosing to outsource can add expertise and augment your security team. It can also provide around-the-clock staffing at a reduced cost to having in-house staff.

Time



Outsourcing eliminates the need to recruit, train and supervise staff on most security operations. It is a good option if you need to have a fully functioning SOC up and running within a short timeframe. However, there is a caveat: MSSPs also face the same hiring challenges you will when it comes to filling and retaining positions, and turnover on their team could also impact your security operation.

Hybrid

This staffing model is a combination of in-house and outsourced employees.

Risk tolerance



With a hybrid model, you get the best of both worlds and some flexibility with how you choose to build your team. You can outsource specialists or highly skilled team members to work during less desirable working hours and keep an in-house team 8x5. This will give your organisation greater coverage and can provide your team with an additional set of eyes on alarms. Another option is to outsource lower-tier staff and keep highly skilled and experienced experts in-house. Outsourcing entry-level tasks can also alleviate some of the impact turnover at an MSSP could have on your operation.

Budget



This staffing model is beneficial if you need a 24x7 SOC operation, but do not have the resources to build one in-house. If you're building a small-to-medium-sized team from the ground up, you can save significant costs by outsourcing to fill skillset gaps.

Time



This model can help you achieve 24x7 coverage quicker than recruiting in-house staff. You have the option to outsource most of your operation, while you take time to recruit and hire in-house personnel.

| Staffing model | Pros | Cons |
|----------------|--|--|
| In-house | <ul style="list-style-type: none"> • Quick communication • Can have higher accuracy • All data is kept internally • Your team can apply their knowledge of the organisation in their work | <ul style="list-style-type: none"> • Generally, the most expensive model • Can take longer to reach maturity • Potential to lose knowledge with a team member • High total cost of ownership to manage a 24x7 operation |
| Outsourced | <ul style="list-style-type: none"> • Service level agreements (SLAs) make the scope and budgeting for the services well-defined • Easy to implement and short ramp up time • Access to 24x7 operations, monitoring, detection and threat intelligence • Reduced operating cost | <ul style="list-style-type: none"> • Difficult to move in-house from this model • MSSPs need time to understand your organisation • Increased risk associated with data being stored outside of your organisation • Requires vendor management |
| Hybrid | <ul style="list-style-type: none"> • Double checking for certain alerts • Your team can get cross-training from experts outside of your organisation • Can help you achieve 24x7 operations without staffing during less desirable times | <ul style="list-style-type: none"> • Model may be costly over time • Increased risk associated with data being stored outside of your organisation • May require you to set up additional hardware |

Figure 1: Pros and cons table for common SOC staffing models

Building your SOC team

Once you select the model that best suits the goals, budget, and risk tolerance of your organisation, the next step will be to add the key roles for your security operation to your hiring strategy. Include descriptions of key roles, who they will report to, qualifications, education, and required skillsets in your strategy to stay consistent with your hiring and serve as a guide to hire the best candidates for your security operation.

An efficient security operation requires fundamental roles and duties to be filled by the right individuals. In addition to a Chief Information Security Officer (CISO) or Chief Information Officer (CIO), your team should include a SOC Manager, Security Engineer(s), Incident Responder(s), and Security Analyst(s). These roles will vary depending on the size and needs of your organisation. Your team may also include skillsets in forensics, malware analysis, and threat intelligence.

The following descriptions will provide an overview of the roles you might include in your hiring strategy. These are some of the essential roles you will find in most security operations; however, they may change based on the structure and size of your team. The names of these roles can also sometimes vary, but the responsibilities are relatively consistent.



Chief Information Security Officer (CISO)

Other titles used include: CSO, VP of Security, Director of Security

The CISO/CSO is a senior-level executive responsible for creating and maintaining a vision and strategy to protect an organisation's information and data security. The role typically requires expert technical knowledge, a bachelor's degree in computer science or a related field, 10+ years of work experience that includes experience in a management role. In addition to technical and industry-specific knowledge, CISOs with an MBA or a background in business will have the skills required to manage a budget, create executable strategies, and communicate on key security metrics and initiatives to a board of executives.

The CISO will often report to directly to the CEO, a member of the C-Suite, or the board in some organisations.

CISO certifications:

CISSP: Certified Information Systems Security Professional

CISM: Certified Information Security Manager

Skillsets and traits to look for in a CISO:

CISOs should have a broad list of technical skills including, but not limited to security technology and architecture, governance, risk, compliance, and experienced in incident response. CISOs will also need to have knowledge of regulatory compliance and compliance assessments. In addition, they need to have the experience business acumen to financially run their organisation and should be experienced in program development.

In addition to technical skills and experience, a CISO should have a dedication to securing an organisation and should display a passion in their commitment to security and show how that they stay up to date on the latest technologies and threats. CISOs are leaders and should be open to providing guidance, training, and growth opportunities.

SOC Manager/Director

Other titles used include: Security Manager, Security Director, SecOps Lead

The SOC Manager or Director is responsible for recruiting, hiring, onboarding, and supervising your security operations team. Smaller organisations may have a SOC Manager who oversees the SOC and reports directly to the CISO, while larger organisations may have a Director role who would oversee the Manager and report to the CISO. A SOC Manager will also create processes to handle security incidents and crisis communication plans, assess incident and compliance reports, measure the SOC performance and report back to business leaders. A SOC Manager should have 5+ years of relevant experience and a bachelor's degree or master's degree in computer science, electrical engineering, or business administration.

The SOC Manager/Director reports to the CISO.

SOC Manager/Director certifications:

CISSP: Certified Information Systems Security Professional

GIAC: Global Information Assurance Certification

GSEC: Global Security Essentials Certification

ISACA: IT Audit, Security, Governance and Risk Certifications

Skillsets and traits to look for in a SOC Manager/Director:

A SOC Manager should be able to demonstrate their ability to manage and optimise security operations programs and have a strong understanding of compliance requirements and crisis management. They should have strong leadership and communication skills and should also be able and willing to assist in security response when needed. He or she should have a passion and understanding for information security, network security, and network hardware.

Security Engineer

Other used titles include: Cybersecurity Engineer, Security Engineer, SIEM Engineer, Technology Engineer

A Security Engineer is responsible for implementing and administrating network security hardware and software and identify any vulnerabilities in systems. He or she will monitor networks and systems to find and resolve potential security threats. The Security Engineer will also develop solutions to mitigate vulnerabilities and document standards for operating procedures and protocols. He or she should have 5+ years of related experience.

The Security Engineer reports to the SOC Manager.

Security Engineer certifications:

CISSP: Certified Information Systems Security Professional

CISM: Certified Information Security Manager

TOGAF: The Open Group Architecture Framework

Axelos ITIL Master Certification

AWS Certified Solution Architect

Skillsets and traits to look for in a Security Engineer:

Security Engineers should have a broad list of technical skills including, but not limited to: VB.NET, Java/J2EE, API/web services, scripting languages (PowerShell), and coding languages (Python, C#, C, Go), knowledge of systems and technology, and knowledge of modern architectures such as cloud and microservices.

Incident Responder

Other used titles include: Incident Handler, Malware Analyst, Forensics Examiner, Threat Intel Analyst

Incident Responders have the knowledge to lead investigations of confirmed incidents and quickly respond to and neutralise threats before they are classified as incidents. He or she will manage and prioritise work during security incidents, including forensics and remediation. He or she will help monitor systems and networks for intrusion and identify security vulnerabilities. They should be experts in your security operation's systems and have skills in forensics, malware analysis, and threat intelligence. Incident Responders typically have a bachelor's degree in computer science and two to three years of related experience.

The Incident Responder will report to the SOC Manager.

Incident Responder certifications:

CCE: Certified Computer Examiner

CEH: Certified Ethical Hacker

GCFE: GIAC Certified Forensic Examiner

GCFA: GIAC Certified Forensic Analyst

GCIH: GIAC Certified Incident Handler

Skillsets and traits to look for in an Incident Responder:

Incident Responders should have a list of technical skills including, but not limited to in-depth knowledge of systems, applications, and systems forensics, an understanding of various coding languages, strong knowledge of threat intelligence, and may be able to reverse engineer malware. Incident responders should be able to work under extreme pressure, be highly adaptable, and have strong analytical and problem-solving skills.

Security Analyst

Other used titles include: SOC Analyst

Security Analysts are one of the most fundamental roles in a SOC. He or she primarily focuses on monitoring the environment, threat detection, and incident response. Most large organisations will employ different levels of Security Analyst starting at triage (level one) and moving up based on expertise to tasks like threat intelligence, forensics, malware analysis, and incident response. Security Analysts may have one to three years of experience.

The Security Analyst reports to the SOC Manager.

Security Analyst Certifications:

CISSP: Certified Information Systems Security Professional

GSEC: GIAC Security Essentials Certification

GCFE: GIAC Certified Forensic Examiner

GCIH: GIAC Certified Incident Handler

Skillsets and traits to look for in a Security Analyst:


Security Analysts should have a list of technical skills including, but not limited to and understanding of sysadmin (Linux/Mac/Windows) and programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more). Security Analysts should show a willingness to learn and enthusiasm about their future in security. A Security Analyst should have experience with ethical hacking and be able to think like a hacker. They should be able to demonstrate their ability to identify threats and know the workflows associated with investigating events and incidents. They should be proactive and problem solvers. Your ideal candidate should possess intellectual curiosity and have a strong desire to find and mitigate risks.

Retaining your security team

Recruiting is only one part of the equation. You need to also have a strategy for retaining and developing top talent.

A (ISC)² study of cybersecurity professionals found that 76 per cent of those surveyed are solicited to change jobs by recruiters at least once a month, and 70 per cent said they are open to new job opportunities this year.

In addition to the constant poaching from recruiters, high turnover rates are also a concern for security teams. According to an ESG research study, 63 per cent of respondents believe the cybersecurity skills shortage has caused an increase in workloads for existing staff.



Average leaders raise the bar on themselves; good leaders raise the bar for others; great leaders inspire to raise their own bar.
— Orrin Woodward

"People don't leave bad companies. People leave bad managers and leaders. To be a leader people want to work for, you should be a servant-leader first. Part of this means setting aside your ego to be strong enough to hire to offset known weaknesses and trust your team," says James Carder, LogRhythm CSO and VP of LogRhythm Labs

The following are things good leaders can do to help combat the common reasons security professionals decide to leave a team:

- **Invest in your employees.** Enable professional and personal growth for your staff by investing in training initiatives, certifications, and opportunities for your team to attend events. Offer salaries that are competitive with the market. You can find salary averages for essential security operations roles in the [SOC job description templates](#).
- **Have your teams' back.** Trust your team, give them autonomy in their work, and help support their decisions. A leader should help their employees prioritise tasks which can mean stepping in if they are being sent too many requests from leaders outside of the security operation. Provide an outlet for your team to speak openly about concerns and show that their concerns are heard and considered.
- **Engage staff and allow for creativity.** Take time to understand your employee's career interests and goals. Allow them to explore security projects that challenge them and provide solutions the rest of the team can benefit from.
- **Create a culture of cybersecurity.** Your team should know how vital their roles are to the safety and longevity of your organisation. Show them that you are a champion for the security program and give the rest of the organisation visibility into the work they are doing. Your team should feel accomplished and that they have contributed to the business in a meaningful way and feel that the rest of the organisation supports the work they are doing.
- **Offer bonuses and extra perks.** Include a plan for how you will reward employees for increasing years of service on your team. Show candidates that you care about your team and offer team building events, awards, and additional perks that consider the importance for work-life balance.

Hire the right people

Retaining your security staff begins with hiring the right candidates in the first place. The cybersecurity skills gap makes it imperative that you hire candidates that are a good fit for your team and organisation — it will be difficult to replace team members if your new hire does not work out. According to an ISACA workforce trends study, 69 per cent of respondents say they are understaffed, and 62 per cent of respondents say that, on average, it takes them three or more months to fill a cybersecurity position.

As said by the famous technologist, business leader, and philanthropist, Bill Gates, “I choose a lazy person to do a hard job. Because a lazy person will find an easy way to do it.” While you might not want to seek out the laziest candidate, you should have a set of qualifying skills and traits that you will use to determine if a candidate will be a good fit for your security operations and organisation. Beyond technical skills, the right candidate should fit well with the culture of your organisation and team. It can be tempting to deviate from your hiring strategy if you find a candidate with solid skills, but try not to deviate from your hiring strategy and make every hire purposeful and aligned with your team and strategy.



Advice from your peers

We polled experts in the field to learn what they look for when hiring a new team member. Here's what they said:

“

I look for candidates who are skilled in incident handling methodologies that can detect host and network-based intrusions using intrusion detection technologies. Being able to apply cybersecurity and privacy principles to organisational requirements related to confidentiality, integrity, availability, authentication, and non-repudiation is also an important hiring consideration.

—Matthew Getzelman, Jimmy Johns

“

The number one skill I look for when hiring, is the ability to think outside the box while still following procedures. Logical thinking and knowledge are also critical skills that you shouldn't overlook.

—Mark Clate, Senior Manager, Managed Services Security Operations, Presidio

“

The top traits I look for when hiring a new security team member are a commitment to the organisation, an inquisitive mind, and an unwavering desire to learn and get ahead.

—Anonymous, Chief Information Security Officer, Services industry

“

What have they done to express their passion for security or a particular part of security? I like to see if they spend any of their free time on research projects or exploring personal initiatives or projects that they are interested in. I look for someone with a passion that fits with the needs of the role and I want to see how their experiences and qualifications align with what they care about.

—James Carder, CSO and VP of LogRhythm Labs

Optimise your job listings

If you are building your security operations in-house or with a hybrid staffing model, then your hiring strategy should include ways your operations will be competitive in the security job market. A good place to start is with job descriptions that will attract the right candidates.

According to a 2018 (ISC)² study on the cybersecurity workforce, 62 per cent of security professionals want to work for an operation with clearly defined roles and responsibilities. Respondents from the same survey said that they view vague job descriptions as a lack of security understanding from the organisation.

Job descriptions should start with clearly defined and differentiable job responsibilities for each role on your team. Your job descriptions and posting should be specific and try to remove ambiguity. Use bullet points and break up text to make it easy for candidates to know what you are looking for and what qualifications are required.

There should be a clear distinction between roles within a SOC, but there will likely be overlap. Flexibility and cross-functional work are a part of life for most security teams, but having clear priorities for each role can help eliminate any friction when employees are asked to step in and assist with tasks outside of their stated duties. Set clear expectations from day one to ensure employees do not feel like you have pulled a bait and switch move on them.

The [SOC job description templates](#) provide sample job descriptions, interview questions, and salary ranges for the essential security operations roles mentioned in this handbook. You can customise these templates to fit the unique needs of your organisation and include them in your hiring strategy.



Next steps

A hiring strategy is critical for building an effective security operation and should be shared with candidates to show the amount of thought you put into building the right team. “Your hiring strategy should serve as your blueprint. If you choose to do so, sharing a hiring strategy with a prospective employee can also show a candidate that you’re thoughtful in building your operation and give them a level of confidence in your leadership abilities,” says Carder.

Your hiring strategy will provide a documented plan for the people side of your security operation and will help you execute on the vision you have for your organisation. Use this handbook as a guide to create a hiring strategy that considers current and future job market challenges, your organisation’s objectives and needs, and how you will attract and keep top talent on your team.

“Strategy execution is the responsibility that makes or breaks executives.”

—Alan Branche and
Sam Bodley-Scott

Carder also notes, “I’ve never been a fan of making exceptions, but that is hard to do in today’s market where the unemployment rate for security professionals is at zero. You might have to make a few calculated exceptions to your hiring plan and should consider revising your strategy as needed.”

You should re-evaluate your strategy from time to time and adjust when appropriate as the needs of your organisation and the job market for security professionals evolves.



Download our [SOC job description templates](#) to help you craft effective job listings for each member of your security team and attract the right candidates.



About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's [award-winning NextGen SIEM Platform](#) delivers comprehensive security analytics; user and entity behaviour analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralisation of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organisations like Cargill, NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organisation each and every day. LogRhythm is the only provider to earn the [Gartner Peer Insights' Customer Choice for SIEM](#) designation three years in a row. To learn more, please visit logrhythm.com.



+44 (0)1628 918 330 // europa@logrhythm.com // Regional HQ, Clarion House,
Norreys Drive, Maidenhead, SL6 4FL, United Kingdom