The SOC Hiring Handbook

Your Guide to Building and Retaining a Strong Security Team

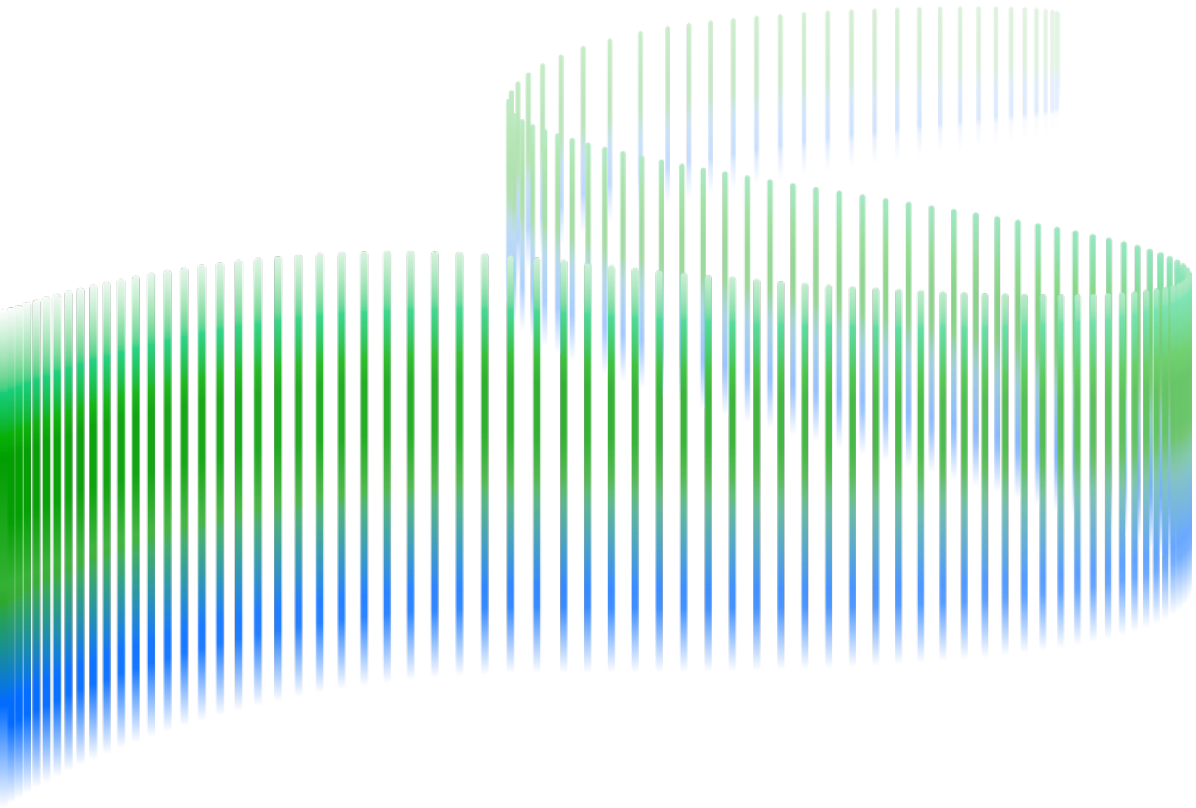


Table of Contents

Building the Backbone of Your Security Operations

A security operations center (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 build an effective security team
- How to plan for your staff while considering staffing models, budget, and organization goals
- What key roles you need on your team and how to find and retain top talent

Overcoming SOC 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 organization.

The Talent Crisis: Finding Skilled Cybersecurity Professionals

Organizations face a significant challenge in finding top cybersecurity talent, with an estimated four million professionals needed to fill the growing workforce gap. As the demand for skilled cybersecurity experts rises due to an expanding attack surface and rapidly evolving threats, most organizations report that this shortage increases their risk exposure. According to Fortinet's 2024 Global Cybersecurity Skills Gap Report, nearly 90% of leaders experienced a breach in the past year that they partially attributed to insufficient cybersecurity skills, highlighting the escalating impact of this talent shortage on organizations' security posture.

Unfortunately, the current state of education and professional development is not adequately addressing the cybersecurity talent shortage. Many educational institutions, including universities and community colleges, are not producing enough graduates with the necessary cybersecurity skills to meet the growing demand. Additionally, many organizations struggle to provide continuous professional development opportunities, leaving employees without the up-to-date training required to handle evolving threats. Without sufficient employer investment in technical training and growth areas like compliance, risk management, and leadership, organizations face increasing difficulty in retaining and advancing their cybersecurity workforce.

Frequent Turnover: Mitigating the Impact on Your SOC

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 number of 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 skill set.

Employee turnover can unbalance workloads, put a damper on morale, and prohibit your team from maturing. According to a Kaspersky report, 48% of organizations say it takes them at least six months to fill open positions. Depending on the size of your security operations, a half-year period without a fully staffed team could put your organization at a higher risk for attacks.

To minimize disruption and adequately protect your organization 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.

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

Crafting a Comprehensive 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, which 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 organization'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.

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 organizations, the SOC Manager oversees hiring for their team because they manage the team and are responsible for their growth, development, and, largely, job satisfaction. The CISO/CSO/CIO should communicate their hiring strategy and budget with their SOC Manager so they can adequately hire candidates who align with the organization's goals.

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

Justifying Your SOC Hiring Budget: Proving the Value of People

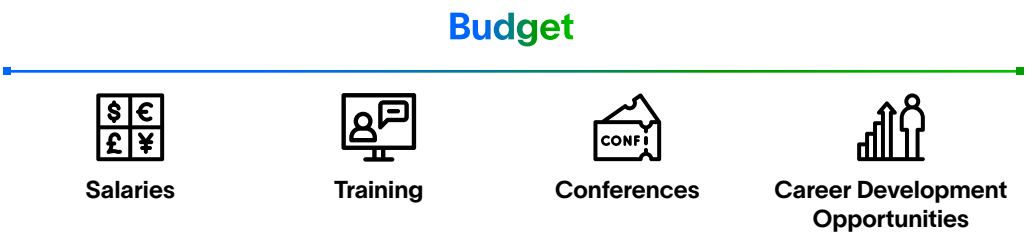
Once you determine the positions you need, the next step is to budget for your team. You will need to convince an executive team and board that you require a budget for your people that is adequate to manage your organization's security risk. Part of reducing the risk of a breach is having essential 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 which are essential 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.

Mapping Out Your Security Operations: Organizational Chart and Staffing Models

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

The structure of a SOC can vary widely. This variation is 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 organizational chart to reflect any changes that can occur as your company scales.



Choosing the Right SOC Staffing Model for Your Needs

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 organization'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 organization
- The level of risk in your industry
- The level of risk your organization is comfortable with
- The industry and the requirements for doing business in that industry for both your organization 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.

In house	Hybrid	Outsourced

Fully In House

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

If your organization 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 the criticality and impact of any alert. If you're building a security team for a large organization with a lower risk tolerance, then a fully in-house model would require you to have 24/7 team coverage.

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

It can take a considerable amount of time to hire and onboard a fully in-house staff. You should consider the level of risk your organization will be under while you build your team and if you will be able to adequately protect your organization while you find and hire staff. If your organization is at 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.

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 organization for the level of risks it tolerates. You will also need to consider how imperative knowledge of your organization or industry is to detect and prevent potential threats. A fully outsourced option is great for organizations that have a low risk tolerance and do not require specialized knowledge related to the organization or its industry.

The decision to hire an outside party to manage security should depend greatly on whether your resources can detect, respond to, 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 lower cost than in-house staff.

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

Hybrid

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

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 staff 8x5. This will give your organization 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.

This staffing model is beneficial if you need a 24/7 SOC operation, but do not have the resources to build one in-house. If you're building a small-to-medium team from the ground up, you can save significant costs by outsourcing to fill skill set gaps.

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

Staffing Model	Pros	Cons
In House	• Quick communication • Can have higher accuracy • All data is kept internally • Your team can apply their knowledge of the organization in their work	• 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 24/7 operation
Outsourced	• Service level agreements (SLAs) make the scope and budgeting for the services well defined • Easy to implement and short ramp-up time • Access to 24/7 operations, monitoring, detection, and threat intelligence • Reduced operating cost	• Difficult to move in house from this model • MSSPs need time to understand your organization • Increased risk associated with data being stored outside of your organization • Requires vendor management
Hybrid	• Double-checking for certain alerts • Your team can get cross training from experts outside of your organization • Can help you achieve 24/7 operations without staffing during less desirable times	• Model may be costly over time • Increased risk associated with data being stored outside of your organization • May require you to set up additional hardware

Building Your SOC Dream Team: Key Roles and Responsibilities

Once you select the model that best suits the goals, budget, and risk tolerance of your organization, 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 skill sets in your strategy to stay consistent with your hiring and serve as a guide to hire the best candidates for your security operations.

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 and depending on the size and needs of your organization. Your team may also include skill sets 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 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 organization'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 often reports directly to the CEO, another member of the C-suite, or, in some organizations, the board.

CISO Certifications:

- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager

Skill Sets 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 experience 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 organization and should be experienced in program development.

In addition to technical skills and experience, a CISO should have a dedication to securing an organization and should display a passion in their commitment to security and demonstrate 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 organizations may have a SOC Manager who oversees the SOC and reports directly to the CISO, while larger organizations may have a Director role who would oversee the Manger 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

Skill Sets and Traits to Look for in a SOC Manager/Director

A SOC Manager should be able to demonstrate their ability to manage and optimize 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 titles include: Cybersecurity Engineer, Security Engineer, SIEM Engineer, Technology Engineer

A Security Engineer is responsible for implementing and administering network security hardware and software and identifying any vulnerabilities in systems. They 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. They 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

Skill Sets 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 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 neutralize threats before they are classified as incidents. He or she will manage and prioritize 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 reports 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

Skill Sets 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 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 organizations 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: Global Security Essentials Certification
- GCFE: GIAC Certified Forensic Examiner
- GCIH: GIAC Certified Incident Handler

Skill Sets 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 Top Talent in a Competitive Market

Recruiting is only one part of the equation. Retention and development of talent are equally important.

The 2023 ISC2 Cybersecurity Workforce Study reports that 75% of cybersecurity professionals find today's threat landscape to be the most difficult in the past five years. The demand for skilled workers remains high, with 92% of organizations citing significant gaps in their cybersecurity teams.

> "Average leaders raise the bar on themselves; **good leaders raise the bar for others; great leaders inspire to raise their own bar."**
>
> - Orrin Woodward

Turnover is another challenge. According to a 2023 Enterprise Strategy Group (ESG) study, 66% of respondents said the cybersecurity skills shortage has increased workloads for current staff. This is due to difficulty in filling roles, leaving teams overworked and under-resourced, which leads to burnout and further turnover.

Here are ways leaders can help retain their security teams:

- **Invest in employees:** Provide professional development opportunities, including training, certifications, and event attendance. Ensure salaries are competitive. You can find salary averages for essential security operations roles in the SOC Job Description Templates.
- **Support your team:** Trust your team, give them autonomy, and step in to help manage workload when necessary. Offer an open forum for expressing concerns.
- **Engage staff and allow for creativity:** Understand your team's goals and allow them to work on projects that challenge them.
- **Foster a security-focused culture:** Show the importance of their roles and ensure the organization supports their efforts.
- **Provide incentives:** Offer bonuses, team-building events, and recognition to encourage long-term commitment and 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 organization; it will be difficult to replace team members if your new hire does not work out.

As the famous technologist, business leader, and philanthropist, Bill Gates said, "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 organization. Beyond technical skills, the right candidate should fit well with the culture of your organization 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.

Crafting Job Listings That Attract the Right Candidates

If you're building an in-house or hybrid security operations team, your hiring strategy must position your organization competitively in the job market. A key step is crafting job descriptions that will attract the right candidates.

The 2023 (ISC)2 Cybersecurity Workforce Study shows that 67% of cybersecurity professionals believe their organizations are understaffed, making it difficult to manage security issues effectively. Undefined roles and responsibilities further complicate the issue. Vague job descriptions contribute to dissatisfaction and hinder the hiring of qualified talent. Clear, structured roles are essential for attracting and retaining skilled professionals in a competitive market.

While there may be overlap between roles in a SOC, clear distinctions and priorities for each position can help reduce friction. Set clear expectations from the start to avoid misunderstandings and ensure employees feel confident in their roles.

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 customize these templates to fit the unique needs of your organization and include them in your hiring strategy.

Building a Future-Proof SOC Hiring Strategy

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.

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 organization. Use this handbook as a guide to create a hiring strategy that considers current and future job market challenges, your organization's objectives and needs, and how you will attract and keep top talent on your team.

You should reevaluate your strategy from time to time and adjust when appropriate as the needs of your organization and the job market for security professionals evolves.

> "Strategy execution is the responsibility **that makes or breaks executives."**
>
> - Alan Branche and Sam Bodley-Scott

Download the Template

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.

Download now

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. High-integrity data ingestion, powerful analytics, and workflow automation power the industry's most advanced self-hosted and cloud-native security operations platform for threat detection, investigation, and response (TDIR). With a history of leadership in SIEM and UEBA, and a legacy rooted in AI, Exabeam empowers global security teams to combat cyberthreats, mitigate risk, and streamline security operations.

exabeam

Learn more at
www.exabeam.com →