Security Operations Center Job Description Templates

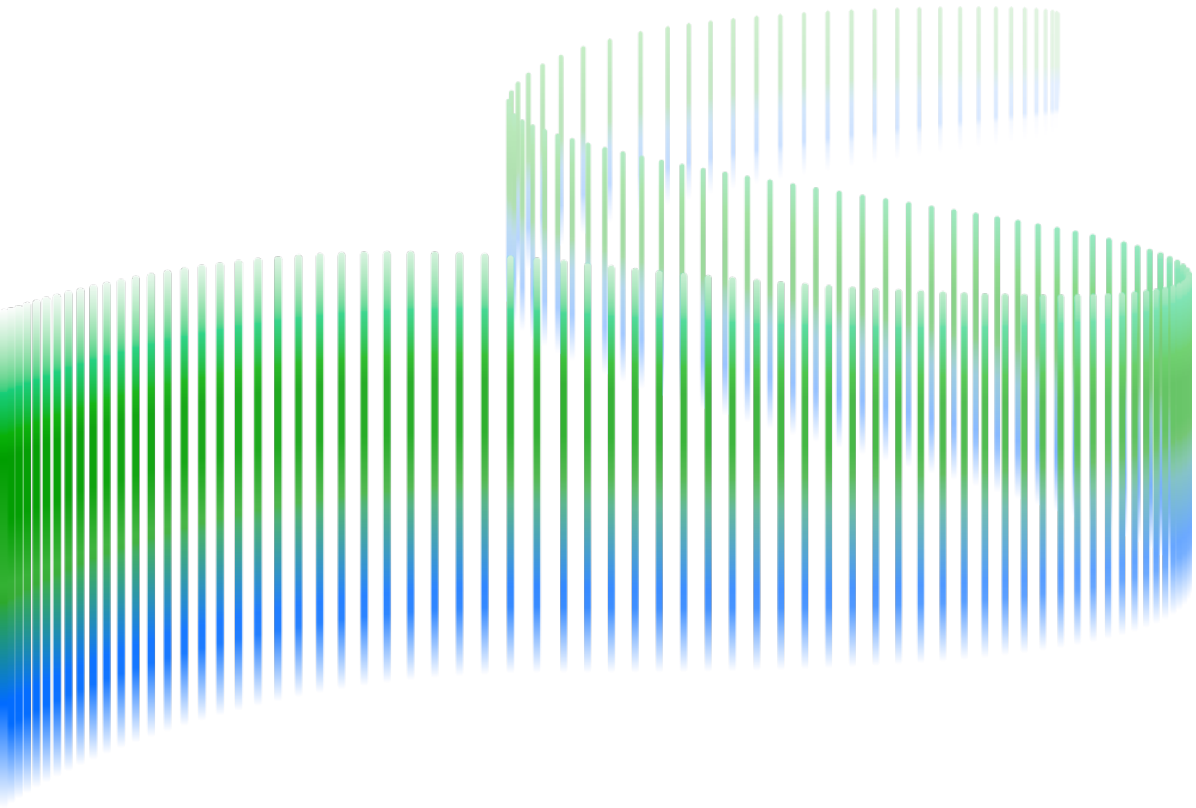

Table of Contents

Introduction

Job descriptions that don't match the actual skills, salary, or experience needed for a cybersecurity role are common issues when hiring security talent. To attract the top security professionals, you will need to create well-written job descriptions with clearly defined roles and responsibilities.

We designed a set of job description templates that you can use, along with the SOC Hiring Handbook, to attract and retain essential security operations roles for your team. The templates provided are designed to serve as a guide to help you craft your own listings and should be customized to fit the unique needs of your organization.

Chief Information Security Officer (CISO) for [Company Name]

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

[Company Name] is seeking a Chief Information Security Officer (CISO) to create and maintain a vison and strategy to protect an organization's information and data security. You will lead operational compliance for standards and regulations for the organization including GDPR, SOC, NYDFS, and others as appropriate. You will drive opportunities to further secure assets and evaluate new and unforeseen threats. This position will work closely with business and IT leaders to define and ensure ongoing adherence to information security policies and standards and will also be responsible for reporting on security KPIs.

Required Qualifications

- 10+ years of IT and relevant security experience
- Bachelor's in Computer Science, Information Security, Business, Management, Information Technology, or related field
- Experience interpreting and applying industry frameworks
- Demonstrated experience working with organization management and ability to interact at executive and board level
- Knowledge of legal and regulatory requirements relating to information security and privacy

Preferred Qualifications

- Master's in Computer Science, Information Security, Business, or related field preferred
- Certifications including but not limited to:
  - CISSP: Certified Information Systems Security Professional
  - CISM: Certified Information Security Manager

Responsibilities

- Establish and maintain the information security vision and programming to include policy creation, training, risk assessment, and security incident response to ensure information assets and technologies are adequately protected
- Analyze and architect complex solutions to information technology cybersecurity threats that relate to confidentiality, integrity, and availability of data and systems

- Provide regular updates to the executive management team on status of company's risk posture and security program
- Organize and lead the security incident response capability, preemptively engaging with and training stakeholders throughout the organization
- Manage and oversee our business continuity and disaster recovery efforts to ensure the organization is prepared for high-risk business disruptions
- Manage and oversee internal and external IT compliance related audit efforts
- Keep abreast of latest security and privacy legislation, regulations, adversaries, alerts, and vulnerabilities
- Develop and manage budget for security related capital and operational expenses, training, and staff needs

Skills

- High level of personal integrity and the ability to professionally handle confidential matters and demonstrate the appropriate level of judgment and maturity in risk decision making
- Demonstrated ability to identify and advocate for investments to achieve the security strategy and provide ROI analyses to recommend new spend as appropriate
- Ability to quickly assess complex situations and take appropriate action, such as during security incidents
- Excellent written and verbal communication skills, interpersonal and collaborative skills, and the ability to communicate security- and risk-related concepts to technical and nontechnical audiences
- Ability to lead and motivate cross-functional, interdisciplinary teams
- Demonstrable evidence of change management skills
- Project management skills, financial/budget management, scheduling, and resource management

Salary Suggestions

- Average: $216,527
- Ranges: $278,000–$476,000

*Salary figures based on data from averages found via Payscale and Glassdoor

Sample Interview Questions:

- Can you provide an example of how you would present information about technical matters in a way that all members of our board would understand?
- Describe the most profound executive decision you have ever made in a related role.
- How would you define a strong security operations program?
- What have you done to expand or improve your knowledge of the information security industry in the last year?

Security Operations Center Manager for [Company Name]

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

[Company Name] is seeking a Security Operations Center (SOC) Manager who will be responsible for leading a team of security analysts. The SOC Manager will provide leadership, coordination, and operational management of the security team. You will play a critical role at **[Company Name]** and lead security personnel, developing strategy, setting goals, and providing performance and professional development feedback. As the SOC Manager, you will lead the security operations team to continually improve the SOC and manage security policies, procedures, and processes.

Required Qualifications

- 5+ years of IT and relevant security experience
- 3+ years of experience leading or serving as a senior member of a security operations team
- Bachelor's in Computer Science, Information Security, Business, Management, Information Technology, or related field
- Knowledge of current and emerging technologies and tactics used within a SOC and how they can be applied to improve efficiency and effectiveness
- Understanding of the information security industry and the current threat landscape

Preferred Qualifications

- Certifications including but not limited to:
  - CISSP: Certified Information Systems Security Professional
  - GIAC: Global Information Assurance Certification
  - GSEC: Global Security Essentials Certification
  - ISACA: IT Audit, Security, Governance, and Risk Certifications
- Prior experience working as a SOC Manager is a plus.

Responsibilities

- Work with the rest of the security operations team to support analysts with performance feedback, training, and career direction
- Assist with screening and hiring security analysts

- Manage and coordinate incident response and forensic processes
- Monitor and enforce guidelines for best practices in security and compliance
- Support routine regulatory and compliance initiatives
- Orchestrate daily compliance requirements and tasks as required

Skills

- Strong leadership skills and the ability to guide others during incident and crisis management
- Able to tune correlation rules and outcomes via security information and event management (SIEM) and security orchestration, automation, and response (SOAR) platforms
- Familiarity with Linux and Windows capabilities and with network- and host-based forensic processes
- Familiarity with the investigation of malware and host compromise incidents
- Understanding of intrusion detection systems, web application firewalls, and IP regulation systems
- Technical understanding of current cybersecurity threats and trends
- Able to multitask, prioritize, and resolve multiple inquiries at once
- Excellent oral and written communication, interpersonal, organizational, and presentation skills

Salary Suggestions

- Average: $101,322
- Ranges: $60,000–$186,000

*Salary figures based on data from averages found via Payscale and Glassdoor

Sample Interview Questions:

- Can you provide an example of a time when you successfully trained team members in security procedures and what methods led to a successful training?
- Can you share a method you have used to ensure that security programs comply with all policies and requirements?
- How would you describe your management style?
- What have you done to expand or improve your knowledge of the information security industry in the last year?

Security Engineer for [Company Name]

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

[Company Name] is seeking a Security Engineer to protect sensitive data and systems from threats by implementing and monitoring the appropriate security controls. In this role, you will assess potential systems and process vulnerabilities to determine security infrastructure requirements, make recommendations, and make changes to enhance systems security. You will develop security policies and procedures and communicate security requirements and procedures to users.

Required Qualifications

- 5+ years of relevant security experience
- Bachelor's in Computer Science, Information Security, Business, Management, Information Technology, or related field
- Previous security experience with a variety of security technologies

Preferred Qualifications

- Certifications including but not limited to:
  - CISSP: Certified Information Systems Security Professional
  - CISM: Certified Information Security Manager
  - ISSAP: Information Systems Security Architecture Professional
  - CEH: Certified Ethical Hacker
  - AWS Certified Solution Architect

Responsibilities

- Identify and document information security risks and propose mitigating controls
- Investigate and respond to security incidents
- Monitor networks and systems for potential threats
- Research, design, and develop new information security controls
- Actively research, evaluate, and drive next-generation security technologies and solutions to solve the organization's needs
- Manage solution development and deployment that adhere to best practices

Skills

- Previously assessed, developed, implemented, operationalized, and documented comprehensive security technologies and processes
- Hands-on experience with multiple security technologies such as antivirus software, intrusion detection, firewalls, and content filtering
- Prior experience with secure software development, data protection, cryptography, key management, identity and access management (IAM)m network security (VPNs) within SaaS, IaaS, PaaS, and other cloud environments
- Solid understanding of a range of compliance, regulatory, and legal requirements and relevant principles, best practices, and standards across multiple industries (for example, PCI, SOX, GLBA, CSA, PCI, NIST, ISO, IEEE, FedRAMP, HIPAA, and TCG)

Salary Suggestions

- Average: $100,781
- Ranges: $69,000–$147,000

*Salary figures based on data from averages found via Payscale and Glassdoor

Sample Interview Questions:

- What type of tests do you use to detect security faults in a network and why?
- Tell me about a time when your ability to analyze needs and product requirements helped you make an informed decision to benefit your company's security.
- What have you done to expand or improve your knowledge of the information security industry in the last year?

Incident Responder for [Company Name]

Other titles include: Incident Manager, SOC Analyst*

* This job description is designed for entry-level or Tier 1 analysts

[Company Name] is seeking an Incident Responder who will be responsible for leading forensics and remediation during security incidents. You will proactively identify security flaws and vulnerabilities and then develop plans of action to remediate those issues. Your goal is to work through security incidents and research to find new ways to surface novel methods of threat detection across a complex organization. The ideal candidate should be able to work under extreme pressure and be a strong problem solver.

Required Qualifications

- 2+ years of relevant security experience
- Bachelor's in Computer Science, Information Security, Business, Management, Information Technology, or related field
- Hands-on experience in the detection, response, mitigation, and/or reporting of cyberthreats affecting networks, computer intrusion detection, analysis, and incident response

Preferred Qualifications

- Certifications including but not limited to:
  - CCE: Certified Computer Examiner
  - CEH: Certified Ethical Hacker
  - GCFE: GIAC Certified Forensic Examiner
  - GCFA: GIAC Certified Forensic Analyst
- Experience working with cloud technologies (AWS, Azure, SaaS, etc.)

Responsibilities

- Detect and respond to malicious behavior on cloud systems, SaaS, workstations, servers, and networks
- Optimize threat detection products for data loss prevention (DLP), security information and event management (SIEM), advanced email protection, endpoint detection and response (EDR), antivirus (AV), cloud security products, intrusion detection systems (IDS), and other industry-standard security technologies

- Review and respond to escalated security events
- Proactively hunt threats within the environment
- Write detection signatures, tune systems/tools, develop automation scripts and correlation rules
- Maintain knowledge of adversary tactics, techniques, and procedures (TTPs)
- Conduct forensic analysis on systems and engage third-party resources as required
- Provide timely and relevant updates to appropriate stakeholders and decision makers

Skills

- Experience in forensics, malware analysis, and threat intelligence
- Ability to understand, modify, and create threat detection rules within a SIEM
- Knowledge and experience with Windows and Linux operating systems
- Experience using Python, Perl, PowerShell, or an equivalent language
- Experience with network forensics and associated toolsets and analysis techniques
- Experience with host-based detection and prevention suites (Microsoft SCEP, Carbon Black EDR, OSSEC, etc.)
- Ability to reverse engineer malware is a plus
- Understanding of log collection and aggregation techniques, Elasticsearch, Logstash, Kibana (ELK), syslog-NG, Windows Event Forwarding (WEF), etc.
- Ability to correlate data from multiple sources to create a more accurate picture of cyberthreats and vulnerabilities

Salary Suggestions

- Average: $101,714
- Ranges: $66,000–$148,000

*Salary figures based on data from averages found via Payscale and Glassdoor

Sample Interview Questions:

- Describe the most difficult incident that you've ever had to respond to and what you learned from it.
- If you had the chance to build your own Computer Security Incident Response Team (CSIRT) how would you start and what would you need?
- Can you describe a time when you leveraged pen tests to stop a threat?
- What have you done to expand or improve your knowledge of the information security industry in the last year?

Security Analyst for [Company Name]

Other titles include: Incident Manager, SOC Analyst*

* This job description is designed for entry-level or Tier 1 analysts

[Company Name] is seeking a Tier 1 Security Analyst who will be responsible for day-to-day security threat monitoring and analysis. You will manage security incidents and review security alerts for compliance and will work with senior analysts on known or suspected security threats. Reporting to our Security Operations Center Manager, you will work on threat intelligence, forensics and incident response that adhere to best practices and recognized control frameworks.

Required Qualifications

- 1-3+ years of relevant security experience
- Bachelor's in Computer Science, Information Security, Business, Management, Information Technology, or related field
- Practical experience with deployment and/or operation of commonly used information security systems

Preferred Qualifications

- Certifications including but not limited to:
  - CISSP: Certified Information Systems Security Professional
  - GCFE: GIAC Certified Forensic Examiner
  - GCIH: GIAC Certified Incident Handler

Responsibilities

- Manage and support log collection, security scanning, intrusion detection, content filtering, and other security-related systems
- Review and triage information security alerts, provide analysis, determine and track remediation, and escalate as appropriate
- Provide support for log management and security information and event management (SIEM) solutions
- Ensure authorized access by investigating improper access, revoking access, reporting violations, and monitoring information requests

- Provide installation, maintenance, upgrades, and troubleshooting of security applications and appliances across all functional departments
- May perform other duties as assigned including work in other areas to cover absences or relief to equalize peak work periods or otherwise balance the workload

Skills

- Strong knowledge of current security threats, techniques, and landscape, and a dedicated and self-driven desire to research and learn more about the information security landscape
- Experience using endpoint detection and response tools
- Experience and knowledge related to the configuration and maintenance of security monitoring and reporting platforms

Salary Suggestions

- Average: $74,394
- Ranges: $53,000–$103,000

*Salary figures based on data from averages found via Payscale and Glassdoor

Sample Interview Questions:

- Can you define what data leakage is and what factors can cause it?
- Why do you want to work in a security operations center?
- What is SQL injection?
- What have you done to expand or improve your knowledge of the information security industry in the last year?

Next Steps

These templates are a starting point to help you create effective job listings for your security team. Use them as a guide and modify them to fit the needs and requirements of your own security team and organization. Add the descriptions to your hiring strategy, to document clear distinctions between roles within your security operations and provide a model for career growth within your team.

Download the Handbook

Download the SOC Hiring Handbook to learn how to create a hiring strategy that considers current and future job market challenges, your organization's objectives and needs, and how to attract and keep top talent on your team.

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 →