**[SOC Manager](https://www.seek.com.au/job/77438883?ref=search-standalone&type=standard&origin=jobTitle" \l "sol=69e8417477ca13c7b55e8765bff4d53c505c29e7" \t "_blank)**

**The Organisation**  
ACME are currently working with a large financial services organisation in their search to appoint a newly created, enterprise level, SOC Manager to ensure the development of robust and resilient defensive function.  
  
**The Role**  
   
This is a unique opportunity for an experienced Senior Manager to really make their mark and join a highly regulated organisation facing substantial threats from adversaries.  
At a high level, the responsibility of this role covers:

* SOC Strategy and Policy Development
* Managing a high performing team
* Security Operations
* Incident Response
* Detection Engineering
* Threat Hunting
* Threat Intelligence
* Practice Manager duties (i.e. reporting etc)
* Budget Management (Opex & Capex)

**About You**  
This role is a true manager role and would suit someone who has experience managing a large environments SOC where the buck has stopped with you.  
    
What experience are we looking for?

* Substantial experience managing an enterprise security operations centre
* Proven experience managing budgets, implementing strategy, uplifting services
* Strong knowledge of cybersecurity principles, threats and defensive tools
* Skilled working with SOC tools such as SIEM, EDR, IDS/IPS and intelligence platforms
* Gravitas and superb communication, problem-solving and decision-making ability

Why would you join?

* True leadership role with the pull to make big decisions
* Work with a leading CISO, peer management group and board that listens
* Work with best of breed technology
* Select a new MSSP and hire the team
* Key project work
* Salary - $240k - $260k package + Up to 20% bonus (OTE $312k)
* Hybrid

# Interview Script

**Interview Question 1: SOC Strategy and Policy Development**

**Interviewer:** "Can you describe your experience in developing SOC strategies and policies?"

**Less Effective Response**

**Interviewee:** "I've been involved in creating some policies and strategies for our SOC. We mostly focused on standard procedures."

**More Effective Response**

**Interviewee:** "In my previous role as a SOC Manager, I led the development of a comprehensive SOC strategy that aligned with our organization's broader cybersecurity objectives. This included establishing clear policies for incident response, threat detection, and compliance with industry standards such as ISO 27001 and NIST. I conducted a thorough risk assessment to identify potential gaps and tailored our strategy to address these vulnerabilities. Additionally, I introduced a continuous improvement plan, incorporating regular reviews and updates to ensure our policies stayed current with the evolving threat landscape. This strategic approach not only strengthened our defensive posture but also improved our team's readiness to handle incidents efficiently."

**Interview Question 2: Managing a High Performing SOC Team**

**Interviewer:** "How have you managed and developed a high-performing SOC team in your previous roles?"

**Less Effective Response**

**Interviewee:** "I've managed SOC teams before. I make sure they know their tasks and support them when needed."

**More Effective Response**

**Interviewee:** "As a SOC Manager, I have focused on building a high-performing team by emphasizing continuous learning and professional development. I implemented a structured training program that included certifications like CISSP and CEH, and encouraged participation in cybersecurity conferences and workshops. I also fostered a collaborative team culture by holding regular team meetings to discuss recent threats, share knowledge, and conduct tabletop exercises. Performance metrics and KPIs were established to measure individual and team performance, ensuring accountability and continuous improvement. This holistic approach not only enhanced the technical skills of the team but also improved morale and cohesion, resulting in a more resilient and effective SOC."

**Interview Question 3: Experience with Incident Response and Detection Engineering**

**Interviewer:** "Can you provide an example of how you've led incident response and detection engineering efforts?"

**Less Effective Response**

**Interviewee:** "I've handled incident responses before. We usually follow a standard procedure to contain and resolve the issue."

**More Effective Response**

**Interviewee:** "In one notable incident, our SOC detected unusual network traffic indicative of a potential data breach. As the SOC Manager, I immediately activated our incident response plan, coordinating efforts across the team to contain the threat. We isolated the affected systems and conducted a root cause analysis, discovering that the breach was caused by a zero-day vulnerability in a third-party application. Simultaneously, our detection engineering team worked on refining our SIEM rules and signatures to detect similar threats in the future. Post-incident, we conducted a thorough review, updating our detection strategies and implementing additional safeguards. This comprehensive approach ensured minimal impact and strengthened our overall security posture."

**Interview Question 4: Budget Management and Strategic Implementation**

**Interviewer:** "How have you managed budgets and implemented strategic initiatives in a SOC environment?"

**Less Effective Response**

**Interviewee:** "I've managed budgets for SOC operations before, mostly focusing on keeping costs down and allocating resources as needed."

**More Effective Response**

**Interviewee:** "In my role as a SOC Manager, I was responsible for managing both Opex and Capex budgets. This involved careful planning and allocation of resources to ensure we had the necessary tools and technologies while maintaining cost efficiency. For instance, I led the initiative to implement a new EDR solution, which required a significant upfront investment but promised long-term cost savings and improved threat detection capabilities. I presented a detailed business case to the board, highlighting the ROI and strategic benefits. Additionally, I managed vendor relationships and negotiated contracts to ensure we received the best value. My strategic budget management enabled us to enhance our SOC capabilities while staying within financial constraints."

**Interview Question 5: Collaboration and Communication with Stakeholders**

**Interviewer:** "How do you communicate and collaborate with key stakeholders, such as the CISO, board members, and external partners?"

**Less Effective Response**

**Interviewee:** "I usually keep stakeholders informed through reports and meetings. I make sure they know what's going on in the SOC."

**More Effective Response**

**Interviewee:** "Effective communication and collaboration with stakeholders are crucial for the success of SOC operations. I regularly brief the CISO and board members on the current threat landscape, key incidents, and our response efforts. I provide detailed reports that include metrics on incident response times, threat detection rates, and ongoing projects. In addition, I collaborate with external partners, such as MSSPs and intelligence providers, to enhance our threat intelligence capabilities. During critical incidents, I ensure transparent and timely communication with all relevant parties, keeping them informed of our actions and any potential impact on the business. This proactive approach builds trust and ensures alignment with organizational goals."

**Interview Question 6: Threat Hunting and Intelligence**

**Interviewer:** "Can you explain your experience with threat hunting and leveraging threat intelligence in a SOC environment?"

**Less Effective Response**

**Interviewee:** "I've been involved in threat hunting and using threat intelligence to stay updated on the latest threats."

**More Effective Response**

**Interviewee:** "In my previous role, I led a dedicated threat hunting team that actively sought out potential threats within our network. We used threat intelligence feeds from multiple sources, including commercial providers and government agencies, to stay ahead of emerging threats. Our approach involved creating custom detection rules in our SIEM and using tools like Splunk and Elastic Stack to analyze network traffic and logs. We also developed hypotheses based on known adversary tactics and techniques, testing these against our environment to uncover any signs of compromise. This proactive threat hunting not only helped us identify and mitigate threats early but also refined our detection capabilities and informed our overall security strategy."

**Interview Question 7: Practice Manager Duties and Reporting**

**Interviewer:** "How have you handled practice management duties, such as reporting and maintaining operational standards in a SOC?"

**Less Effective Response**

**Interviewee:** "I prepare reports and ensure that our SOC meets its standards. I also handle day-to-day management tasks."

**More Effective Response**

**Interviewee:** "As a SOC Manager, I have been responsible for overseeing all practice management aspects, including regular reporting and maintaining high operational standards. I implemented a comprehensive reporting system that tracks key performance indicators (KPIs) such as incident response times, false positive rates, and system uptime. These reports were shared with senior management and used to drive continuous improvement. Additionally, I developed and maintained standard operating procedures (SOPs) to ensure consistency in our response processes and adherence to best practices. I also conducted regular reviews and audits to identify areas for improvement and ensure compliance with regulatory requirements. This structured approach ensured that our SOC operated efficiently and effectively."

**Interview Question 8: Experience with SOC Tools and Technologies**

**Interviewer:** "What SOC tools and technologies are you most familiar with, and how have you used them to enhance security operations?"

**Less Effective Response**

**Interviewee:** "I've used various SOC tools like SIEMs and EDRs. They're important for monitoring and responding to threats."

**More Effective Response**

**Interviewee:** "I have extensive experience with a range of SOC tools and technologies, including SIEM platforms like Splunk and ArcSight, EDR solutions such as CrowdStrike and Carbon Black, and IDS/IPS systems like Snort and Suricata. These tools are integral to our security operations, enabling us to monitor network traffic, detect anomalies, and respond to incidents promptly. For example, I configured custom dashboards and alerts in Splunk to track critical security events, which helped us quickly identify and address potential threats. I also worked on integrating threat intelligence feeds into our SIEM to enrich our data and improve threat detection accuracy. This comprehensive use of SOC tools allowed us to maintain a robust security posture and quickly adapt to evolving threats."

**Interview Question 9: Handling Budget Management in a SOC**

**Interviewer:** "Can you discuss your experience in managing budgets for a SOC, including both Opex and Capex?"

**Less Effective Response**

**Interviewee:** "I've been involved in managing SOC budgets, focusing on allocating resources and managing expenses."

**More Effective Response**

**Interviewee:** "In my role as a SOC Manager, I was responsible for managing both operational (Opex) and capital (Capex) budgets. This involved planning and allocating resources for ongoing expenses, such as software licenses, staffing, and training, as well as for capital expenditures like hardware upgrades and new tool acquisitions. I developed detailed budget forecasts based on our strategic goals and worked closely with finance to monitor spending and adjust allocations as needed. I also conducted cost-benefit analyses for proposed projects, ensuring that we invested in solutions that provided the best return on investment. This meticulous budget management enabled us to enhance our SOC capabilities while maintaining financial discipline."

**Interview Question 10: Selecting a Managed Security Service Provider (MSSP)**

**Interviewer:** "How have you approached the selection and management of a Managed Security Service Provider (MSSP)?"

**Less Effective Response**

**Interviewee:** "I've been involved in selecting an MSSP before. We reviewed several options and chose the best one."

**More Effective Response**

**Interviewee:** "Selecting and managing a Managed Security Service Provider (MSSP) requires a careful evaluation process to ensure they meet our security needs. I led a comprehensive RFP process, defining our requirements based on factors like the scope of services, response times, reporting capabilities, and compliance with industry standards. We evaluated several providers based on their technical capabilities, customer service, and track record in handling similar environments. After selecting the MSSP, I established a clear service level agreement (SLA) to outline expectations and performance metrics. Regular review meetings were scheduled to assess the MSSP's performance, address any issues, and discuss opportunities for service improvement. This rigorous approach ensured that our partnership with the MSSP effectively supported our security operations."