United Arab Emirates Jobs Expertini®

Senior Engineer - SOC [Splunk]

Apply Now

Company: CPX Holding

Location: abu dhabi

Category: other-general

The SOC Senior Engineer, Splunk, is a critical role responsible for delivering SIEM management services, particularly focusing on Splunk, within the Security Operations Center (SOC). Working closely with the SOC Principal Engineer, SIEM, this role encompasses onboarding new log sources, enhancing and optimizing telemetry, ensuring system updates, resolving issues, and maintaining SIEM performance according to best practices. Reporting to the Director SOC Engineering & Architecture, the SOC Senior Engineer, Splunk, is a professional with a solid foundation in SOC operations.Key ResponsibilitiesDeliver Splunk SIEM management services within the SOC environment.Collaborate with the SOC Principal Engineer, SIEM, in onboarding new log sources to the SIEM platform.Maintain and govern SOC critical log sources, ensuring their proper functionality and integration with Splunk SIEM.Detect log source issues, coordinate with customers to diagnose and resolve them in a timely manner.Enhance and optimize telemetry within the Splunk environment to improve data collection, correlation, and reporting.Perform regular system updates to ensure Splunk functionality and security are up to date.Resolve Splunk-related issues promptly and efficiently.Maintain the performance of the Splunk SIEM according to established best practices.Participate in continuous process improvements to increase SOC efficiency and effectiveness.Provide regular and accurate reports on Splunk services and SOC operations to relevant stakeholders.Contribute to SOC architecture strategy and implementation initiatives related to Splunk.Assist in the mentorship and development of junior SOC engineers.Job SpecificationsSkills:Profound knowledge and hands-on experience with Splunk SIEM and other related technologies like CRIBL.Strong understanding of cloud and network technologies, essential for efficient log source onboarding.Proven technical capabilities in a complex, fast-paced SOC environment.Ability to diagnose and troubleshoot log source issues related to cloud and network infrastructures.Strong understanding of SOC operations, cybersecurity principles, and best practices.Excellent problem-solving skills and the ability to make decisions under pressure.Ability to collaborate effectively with a variety of team members, including interfacing with customers to resolve issues.High proficiency in written and verbal communicationCertifications:Certified Information Systems Security Professional (CISSP), preferred.Certified Information Security Manager (CISM), preferred.Splunk Certified Architect or Splunk Certified Administrator.Cloud-related certifications like AWS Certified Solutions Architect, Google Professional Cloud Architect, or Microsoft Certified: Azure Solutions Architect Expert.Networking certifications such as CCNA or CCNP are advantageous.Educational Experience:Bachelor’s degree in computer science, Information Technology, Cybersecurity, or a related field.A minimum of 5 years of experience in SOC operations, with significant experience in Splunk SIEM management.Prior experience in a technical role within a SOC or similar cybersecurity environment.Apply Now Name * Contact No.* Email address* Years of relevant experience * Resume * (File types : .pdf | File size : up to 5 MB)Cover Letter * (File types : .pdf | File size : up to 5 MB)

#J-18808-Ljbffr

Apply Now

Cross References and Citations:

1. Senior Engineer - SOC [Splunk] AttorneyjobsJobs abu dhabi Attorneyjobs↗

2. Senior Engineer - SOC [Splunk] TruckjobsnearmeJobs abu dhabi Truckjobsnearme↗

3. Senior Engineer - SOC [Splunk] Teachingassistantjobs Jobs abu dhabi Teachingassistantjobs ↗

4. Senior Engineer - SOC [Splunk] Dairyjobs Jobs abu dhabi Dairyjobs ↗

5. Senior Engineer - SOC [Splunk] RiskmanagementjobsJobs abu dhabi Riskmanagementjobs↗

6. Senior Engineer - SOC [Splunk] Legaljobs Jobs abu dhabi Legaljobs ↗

7. Senior Engineer - SOC [Splunk] Unitedarabemiratesjobs Jobs abu dhabi Unitedarabemiratesjobs ↗

8. Senior Engineer - SOC [Splunk] Spainjobs Jobs abu dhabi Spainjobs ↗

9. Senior Engineer - SOC [Splunk] Switzerlandjobs Jobs abu dhabi Switzerlandjobs ↗

10. Senior Engineer - SOC [Splunk] Shanghaijobs Jobs abu dhabi Shanghaijobs ↗

11. Senior Engineer - SOC [Splunk] Oslojobs Jobs abu dhabi Oslojobs ↗

12. Senior Engineer - SOC [Splunk] Internjobs Jobs abu dhabi Internjobs ↗

13. Senior Engineer - SOC [Splunk] Iraqjobs Jobs abu dhabi Iraqjobs ↗

14. Senior Engineer - SOC [Splunk] Businessjobs Jobs abu dhabi Businessjobs ↗

15. Senior Engineer - SOC [Splunk] Italyjobs Jobs abu dhabi Italyjobs ↗

16. Senior Engineer - SOC [Splunk] Hondurasjobs Jobs abu dhabi Hondurasjobs ↗

17. Senior Engineer - SOC [Splunk] Searchnzjobs Jobs abu dhabi Searchnzjobs ↗

18. Senior Engineer - SOC [Splunk] Servicemanagementjobs Jobs abu dhabi Servicemanagementjobs ↗

19. Senior engineer - soc [splunk] Jobs Abu dhabi ↗

20. AMP Version of Senior engineer - soc [splunk] ↗

21. Senior engineer - soc [splunk] Abu dhabi Jobs ↗

22. Senior engineer - soc [splunk] Jobs Abu dhabi ↗

23. Senior engineer - soc [splunk] Job Search ↗

24. Senior engineer - soc [splunk] Search ↗

25. Senior engineer - soc [splunk] Find Jobs ↗

Source: https://ae.expertini.com/jobs/job/senior-engineer-soc-splunk--abu-dhabi-cpx-holding-1968-29219/

Generated on: 2024-05-02 by Expertini.Com