SOC Analyst

Apply Now

Company: QUADRON Cybersecurity Services cPLC

Location: abu dhabi

Category: other-general

QUADRON Cybersecurity Services - SAFETY: CONFIRMED Home >> Careers >> SOC Analyst Careers description SOC ANALYST Type of job : Full Time Seniority level : Junior Line manager : Managing Director Middle East & Africa Join our team in Abu Dhabi as a SOC Analyst! A Splunk SOC (Security Operations Center) Analyst Level 1 is responsible for monitoring and analyzing security events and incidents within an organization's IT infrastructure using the Splunk platform. Their primary role is to ensure the security and integrity of systems, networks, and data. Task & responsibilities The job description of a Splunk SOC Analyst Level 1 typically includes the following responsibilities: - Monitoring: Continuously monitor security events, alerts, and logs generated by various systems, including network devices, servers, and applications, using Splunk or other security information and event management (SIEM) tools. - Incident Detection and Triage: Identify and investigate potential security incidents based on the analysis of log data, network traffic, and other relevant security information. Assess the severity and potential impact of incidents and escalate them to the appropriate teams or higher-level analysts when necessary. - Alert Analysis: Analyze security alerts generated by intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus systems, and other security tools. Determine the validity and relevance of alerts and take appropriate actions as per established procedures. - Incident Response: Assist in the execution of incident response procedures during security incidents. This may involve coordinating with other IT teams, security personnel, or third-party vendors to contain, mitigate, and resolve security incidents. - Documentation and Reporting: Document incident details, investigation findings, and

resolution steps accurately and in a timely manner. Prepare reports and summaries for management and other stakeholders on security incidents, trends, and emerging threats. - Security Event Analysis: Perform in-depth analysis of security events and trends to identify potential security weaknesses, vulnerabilities, or gaps in the existing security infrastructure. Provide recommendations for improving security controls and practices.- Security Tool Management: Assist in the management and maintenance of security tools, including Splunk or other SIEM solutions. This may involve fine-tuning security rules, creating dashboards and reports, and ensuring the proper functioning of security systems.- Security Policies and Procedures: Adhere to established security policies, procedures, and best practices. Stay up to date with the latest security trends, vulnerabilities, and attack techniques to enhance the effectiveness of security monitoring and incident response activities.- Collaboration and Communication: Collaborate with cross-functional teams, including IT operations, network engineering, application development, and security teams, to ensure effective coordination and response to security incidents. Communicate effectively with stakeholders regarding incident updates and mitigation strategies. - Continuous Improvement: Actively participate in training programs and professional development activities to enhance knowledge and skills related to information security, incident response, and the use of Splunk or other security tools. Required skills & experience - Min. 1-3 years of relevant experience What we offer- Home office possibility - Career growth and training opportunities- Challenging and rewarding work assignments APPLY NOW

#J-18808-Ljbffr

Apply Now

Cross References and Citations:

1. SOC AnalystVietnamjobs Jobs abu dhabi   Vietnamjobs ↗

2. SOC AnalystEcommercejobopportunities   Jobs abu dhabi   Ecommercejobopportunities ↗

3. SOC AnalystFilmjobsJobs abu dhabi   Filmjobs ↗

4. SOC AnalystRecruitmentjobs Jobs abu dhabi   Recruitmentjobs ↗

5. SOC AnalystDelhijobs Jobs abu dhabi Delhijobs ↗

6. SOC AnalystSoftwarejobsJobs abu dhabi Softwarejobs↗

7. SOC AnalystSeekingjobs Jobs abu dhabi Seekingjobs ↗

8. SOC AnalystSchoolcounselorjobsJobs abu dhabi Schoolcounselorjobs↗

9. SOC AnalystFindfreelancerjobs Jobs abu dhabi Findfreelancerjobs ↗

10. SOC Analyst Warehousejobsnearme Jobs abu dhabi Warehousejobsnearme↗

11. SOC Analyst FlightattendantjobsJobs abu dhabi Flightattendantjobs↗

12. SOC Analyst Asiajobscareers Jobs abu dhabi Asiajobscareers ↗

13. SOC Analyst FindurgentjobsJobs abu dhabi Findurgentjobs↗

14. SOC Analyst FindparttimejobsJobs abu dhabi Findparttimejobs↗

15. SOC Analyst Videoplatformjoblistings Jobs abu dhabi Videoplatformjoblistings ↗

16. SOC Analyst TextilejobsJobs abu dhabi Textilejobs↗

17. SOC Analyst Barcelonajobs Jobs abu dhabi Barcelonajobs ↗

18. SOC Analyst Thecareerjobs Jobs abu dhabi Thecareerjobs ↗

19. Soc analyst Jobs Abu dhabi ↗

20. AMP Version of Soc analyst ↗

21. Soc analyst Abu dhabi Jobs ↗

22. Soc analyst JobsAbu dhabi ↗

23. Soc analyst Job Search ↗

24. Soc analyst Search ↗

25. Soc analyst Find Jobs ↗