United Kingdom Jobs Expertini®

DevSecOps Engineer

Apply Now

Company: Black Pen Recruitment

Location: London

Category: computer-and-mathematical

Our Client is the largest and only licensedon/offramp platform for stablecoins in Africa. They are dedicatedto offering innovative solutions in the African stablecoins space.Our client is committed to making stablecoins accessible andunderstandable for everyone providing their customers with secureand userfriendly platforms for their financialtransactions.

JobType: Fulltime IRemote

Requirements

- Bachelors degree inComputer Science Information Technology or relateddiscipline
- AWS Certified Security SpecialtyCertified
- CISSP or other industry recognizedcyber security certification preferred
- 5 yearsof experience in AWS cloud infrastructure with a focus on cybersecurity
- 3 years of SOC/IR experience includingincident response triage threat hunting digital forensics andconfiguring alerting rules
- 5 years ofexperience in AWS cloud infrastructure with a focus on cybersecurity
- 3 years of SOC/IR experience includingincident response triage threat hunting digital forensics andconfiguring alerting rules
- Experience workingwithin a Security Operations Center (SOC) including the ability

tobuild purposeful dashboards rules and monitors that contribute toeffective threat detection andresponse.

Experience with AWS Serverlessarchitecture and resources.

Experience with AWSKubernetes.

Experience working in a fullycloudbased fintech company.

Demonstrateproficiency in AWS Security with handson experience in SQS SNS IAMLambda API Gateway S3 DynamoDB Cognito CloudTrail and StepFunctions.

Indepth knowledge of securityconcepts such as cyberattacks and techniques threat vectors riskmanagement incident management etc.

Utilizeand incorporate MITRE ATTACK Framework and Cyber KillChain

Working knowledge of securitytechnologies such as: SIEM EDR FW AD IPS SOAR WAF CTI Applicationand Email Defense Sandbox

Utilize Datadog asboth a SOC and incident management platform leveraging itscapabilities to enhance security operations.

Proficiency in incident management highlighting handson experiencein handling security incidents from identification toresolution.

Experience in threat modeling forAWS services infrastructure and SaaS applications ingeneral

Experience in adhering to compliancestandards specifically ISO27001 andSOC2

Fluency in spoken and writtenEnglish

Ability to perform deep diveinvestigations from start to finish of a securityincident

Capability in securing a data pipelineemphasizing your expertise in monitoring for suspicious activitiesand implementing effective security controls throughout the datalife cycle.

Demonstrate a selfstarter mentalitycollaboration skills sense of urgency strong

attention to detailand ability to operate in a customerorientedenvironment

Exhibit a proactive mindsetshowcasing your ability to identify problems gaps and activelyresearch potential solutions and initiatives to enhance securitymeasures.

Team player open to assisting otherteams and team members within a startupenvironment

Capable of assuming responsibilityfor assigned tasks and seeing them through to completion while alsoadept at extracting new projects or lessons learned from theundertaken work.

Proficient in establishing asystematic approach to sharing knowledge with team membersoperating within the same functionalarea.

Responsibilities

Performrealtime alert monitoring across our cloud Infrastructure andbusiness systems

Swiftly triage and respond tothreats

Initiate and track complexmultithreaded investigations toresolution

Timely support for all Identity andAccess Management requests

Stay up to date withand report on information security issues and emergingtrends

Integrate and share informationeffectively with other analysts andteams

Creation of reports dashboards KPIsmetrics for SOC operations

Assist securityoperations and engineering team whereneeded

Develop documentation and operationalplaybooks as well as suggest alert enhancements to improvedetection capability

Identify gaps in processesand procedures defining solutions escalating to appropriate teamsand supporting implementation to promote consistency in servicedelivery.

Develop and integrate monitoring anddetective capabilities through technologies such as DLP MDMetc.

Develop SIEM use cases for monitoringinvestigative techniques and health checks for optimization andassurance of logging all requiredsystems

Monitor the functioning of securitysystems to ensure the system operates in conformance with expectedperformance and specifications

Evaluate SOCoperating procedures for operational efficiencies and updates tomonitoring rules and use cases

Develop ways tooptimize or automate processes

Create andmodify security SIEM dashboards to clearly identify scope offindings or monitor activity

Provide expertanalysis investigative support of large scale and complex securityincidents and in many cases identify incidents for which atechnical detection may not be available.

Exudeyour upbeat energy and enthusiasm each and every day to motivateyour team to be the best they can in every aspect of what theydo

Celebrate the success of others byrecognising the contributions of committed team members and theirachievements

Align your values with the MissionVision and Values of our clients team

Be a rolemodel for the our clients organizational culture by creating apositive impact at every touchpoint with people with every word yousay or put in print and everything youdo

Communicate in a fashion that is respectfuland well understood

Collaborate with your peersto collectively think of innovative ideas that drive businessthrough technology

Build and utilize workingrelationships with internal business partners across theorganization and external businesscontacts

Remote Work :

No

Apply Now

Cross References and Citations:

1. DevSecOps EngineerSeekingjobs Jobs London Seekingjobs ↗
2. DevSecOps EngineerSeojobs Jobs London Seojobs ↗
3. DevSecOps EngineerKazakhstanjobs Jobs London Kazakhstanjobs ↗
4. DevSecOps EngineerMunichjobs Jobs London Munichjobs ↗
5. DevSecOps EngineerFindurgentjobs Jobs London Findurgentjobs ↗
6. DevSecOps EngineerTeacherjobs Jobs London Teacherjobs ↗
7. DevSecOps EngineerGreecejobs Jobs London Greecejobs ↗
8. DevSecOps EngineerMakkahjobs Jobs London Makkahjobs ↗
9. DevSecOps EngineerSearchukjobs Jobs London Searchukjobs ↗
10. DevSecOps Engineer Neurologistjobs Jobs London Neurologistjobs ↗
11. DevSecOps Engineer Algeriajobs Jobs London Algeriajobs ↗
12. DevSecOps Engineer Craigsjobs Jobs London Craigsjobs ↗
13. DevSecOps Engineer Africajobscentral Jobs London Africajobscentral ↗
14. DevSecOps Engineer Industryjobsearch Jobs London Industryjobsearch ↗
15. DevSecOps Engineer Universityjobsnearme Jobs London Universityjobsnearme ↗
16. DevSecOps Engineer Dominicanrepublicjobs Jobs London Dominicanrepublicjobs ↗
17. DevSecOps Engineer Chefjobsnearme Jobs London Chefjobsnearme ↗
18. DevSecOps Engineer Entryleveljobs Jobs London Entryleveljobs ↗
19. Devsecops engineer Jobs London ↗
20. AMP Version of Devsecops engineer ↗
21. Devsecops engineer London Jobs ↗
22. Devsecops engineer Jobs London ↗
23. Devsecops engineer Job Search ↗
24. Devsecops engineer Search ↗
25. Devsecops engineer Find Jobs ↗