Ghana Jobs Expertini®

Security Operation CentreAnalyst

Apply Now

Company: Black Pen Recruitment

Location: Accra

Category: other-general

Our Client is the largest and only licensed on/off-ramp platform for stablecoins in Africa. They are dedicated to offering innovative solutions in the African stablecoins space. Our client is committed to making stablecoins accessible and understandable for everyone, providing their customers with secure and user-friendly platforms for their financial transactions.

Job Type: Full-time I Remote

Requirements

- Bachelors degree in Computer Science, Information Technology or related discipline
- AWS Certified Security - Specialty Certified
- CISSP or other industry recognized cyber security certification preferred
- 5+ years of experience in AWS cloud infrastructure with a focus on cyber security
- 3+ years of SOC/IR experience, including incident response triage, threat hunting, digital forensics, and configuring alerting rules
- 5+ years of experience in AWS cloud infrastructure with a focus on cyber security
- 3+ years of SOC/IR experience, including incident response triage, threat hunting, digital forensics, and configuring alerting rules
- Experience working within a Security Operations Center (SOC), including the ability to build purposeful dashboards, rules, and monitors that contribute to effective threat

detection and response.

Experience with AWS Serverless architecture and resources.

Experience with AWS Kubernetes.

Experience working in a fully cloud-based fintech company.

Demonstrate proficiency in AWS Security with hands-on experience in SQS, SNS, IAM, Lambda, API Gateway, S3, DynamoDB, Cognito, CloudTrail, and Step Functions.

In-depth knowledge of security concepts such as cyber-attacks and techniques, threat vectors, risk management, incident management, etc.

Utilize and incorporate MITRE ATTACK Framework and Cyber Kill Chain

Working knowledge of security technologies such as: SIEM, EDR, FW, AD, IPS, SOAR, WAF, CTI, Application and Email Defense, Sandbox

Utilize Datadog as both a SOC and incident management platform, leveraging its capabilities to enhance security operations.

Proficiency in incident management, highlighting hands-on experience in handling security incidents from identification to resolution.

Experience in threat modeling for AWS services' infrastructure and SaaS applications in general,

Experience in adhering to compliance standards, specifically ISO27001 and SOC2

Fluency in spoken and written English

Ability to perform deep dive investigations from start to finish of a security incident

Capability in securing a data pipeline, emphasizing your expertise in monitoring for suspicious activities and implementing effective security controls throughout the data life cycle.

Demonstrate a self-starter mentality, collaboration skills, sense of urgency, strong attention to detail, and ability to operate in a customer-oriented environment

Exhibit a proactive mindset, showcasing your ability to identify problems, gaps, and actively research potential solutions and initiatives to enhance security measures.

Team player open to assisting other teams and team members within a startup environment

Capable of assuming responsibility for assigned tasks and seeing them through to completion, while also adept at extracting new projects or lessons learned from the undertaken work.

Proficient in establishing a systematic approach to sharing knowledge with team members operating within the same functional area.

Responsibilities

Perform real-time alert monitoring across our cloud Infrastructure and business systems

Swiftly triage and respond to threats

Initiate and track complex, multithreaded investigations to resolution

Timely support for all Identity and Access Management requests

Stay up to date with and report on information security issues and emerging trends

Integrate and share information effectively with other analysts and teams

Creation of reports, dashboards, KPIs, metrics for SOC operations

Assist security operations and engineering team where needed

Develop documentation and operational playbooks, as well as suggest alert enhancements to improve detection capability

Identify gaps in processes and procedures, defining solutions, escalating to appropriate teams, and supporting implementation to promote consistency in service delivery.

Develop and integrate monitoring and detective capabilities through technologies such as DLP, MDM etc.

Develop SIEM use cases for monitoring, investigative techniques, and health checks for optimization and assurance of logging all required systems

Monitor the functioning of security systems to ensure the system operates in conformance with expected performance and specifications

Evaluate SOC operating procedures for operational efficiencies and updates to monitoring rules and use cases

Develop ways to optimize or automate processes

Create and modify security SIEM dashboards to clearly identify scope of findings, or monitor activity

Provide expert analysis investigative support of large scale and complex security incidents, and in many cases identify incidents for which a technical detection may not be available.

Exude your upbeat energy and enthusiasm each and every day to motivate your team to be the best they can in every aspect of what they do

Celebrate the success of others by recognising the contributions of committed team members and their achievements

Align your values with the Mission, Vision and Values of our clients team

Be a role model for the our clients organizational culture by creating a positive impact at every touchpoint with people, with every word you say or put in print and everything you do

Communicate in a fashion that is respectful and well understood

Collaborate with your peers to collectively think of innovative ideas that drive business through technology

Build and utilize working relationships with internal business partners across the organization and external business contacts

Apply Now

Cross References and Citations:

1. Security Operation Centre Analyst Botanyjobs Jobs Accra Botanyjobs ↗
2. Security Operation Centre Analyst Advertisingjobs Jobs Accra Advertisingjobs ↗
3. Security Operation Centre Analyst Topjobsearch Jobs Accra Topjobsearch ↗
4. Security Operation Centre Analyst Australiacareers Jobs Accra Australiacareers ↗
5. Security Operation Centre Analyst InstallationjobsJobs Accra Installationjobs↗
6. Security Operation Centre Analyst Nutritionistjobs Jobs Accra Nutritionistjobs ↗
7. Security Operation Centre Analyst Chinajobs Jobs Accra Chinajobs ↗
8. Security Operation Centre Analyst Govcareer Jobs Accra Govcareer ↗
9. Security Operation Centre Analyst Digitaljobsnearme Jobs Accra Digitaljobsnearme ↗
10. Security Operation Centre Analyst Dataanalyticsjobs Jobs Accra Dataanalyticsjobs ↗
11. Security Operation Centre Analyst UnitedstatesjobsJobs Accra Unitedstatesjobs↗
12. Security Operation Centre Analyst JavajobsJobs Accra Javajobs↗
13. Security Operation Centre Analyst SearchaustralianjobsJobs Accra Searchaustralianjobs↗
14. Security Operation Centre Analyst Searcheuropeanjobs Jobs Accra Searcheuropeanjobs ↗
15. Security Operation Centre Analyst Chefjobsnearme Jobs Accra Chefjobsnearme ↗
16. Security Operation Centre Analyst Warehousejobsnearme Jobs Accra Warehousejobsnearme↗
17. Security Operation Centre Analyst ProtectiveservicejobsJobs Accra Protectiveservicejobs↗
18. Security Operation Centre Analyst AustinjobsJobs Accra Austinjobs↗
19. Security operation centre analyst Jobs Accra ↗
20. AMP Version of Security operation centre analyst ↗
21. Security operation centre analyst Accra Jobs ↗
22. Security operation centre analyst JobsAccra ↗
23. Security operation centre analyst Job Search ↗

24. **Security operation centre analyst Search ↗**

25. **Security operation centre analyst Find Jobs ↗**

Source: https://gh.expertini.com/jobs/job/security-operation-centre-analyst-accra-black-pen-recruitmen-1584713/

Generated on: 2024-04-30 by Expertini.Com