Storm Lomax

Cloud Engineer & Security Specialist

07933163485
stormlomax@icloud.com
linkedin.com/in/stormlomax
github.com/stormlomax

EXPERIENCE

SSE PLC, Glasgow — *Cloud Engineer*

FEBRUARY 2025 - PRESENT

- Worked in the Site Reliability Engineering space to maintain high availability of cloud services and performance, including providing support, advice, and increasing automation.
- Managed firewall requests to ensure secure network configurations and compliance.
- Created and managed network security groups to control inbound and outbound traffic.
- Conducted detailed searches of firewall logs for effective troubleshooting and incident resolution.
- Oversaw identity and access management processes to protect sensitive information.
- Utilised Terraform for infrastructure as code (IaC) to automate cloud resource provisioning.
- Employed Visual Studio Code for efficient coding and project management.
- Handled cloud maintenance support tickets to address and resolve technical issues.
- Utilised ServiceNow for incident management and tracking of support requests.
- Gained cross-cloud experience working with both Azure and AWS environments.
- Implemented CI/CD pipelines using GitHub for streamlined application deployment.
- Developed automation scripts using Python and PowerShell to enhance operational efficiency.

NatWest, Edinburgh — *Cyber Security Apprentice*

OCTOBER 2023 - FEBRUARY 2025

- Utilising security tools such as HashiCorp Vault to provision namespaces for secrets management. Required knowledge of Git and Terraform to build namespaces and push branches, as well as collaboration with colleagues and internal customers.
- Managed compliance frameworks such as SOC 2, ISO27001 and PCI DSS.

SOFTWARE AND TOOLS PROFICIENCY

Microsoft Azure

AWS

Terraform

Git CI/CD

Splunk

HashiCorp Vault

Visual Studio Code

ServiceNow

CERTIFICATIONS

Terraform Associate
HashiCorp Cloud
Dec 2024

AWS Certified Cloud Practitioner
Amazon AWS
July 2024

Level 5 CIPD in People Management
CIPD
Sept 2023

LANGUAGES

Lorem ipsum, Dolor sit amet, Consectetuer

- Utilised risk management processes, including risk identification, assessment and mitigation.
- Creating additional functionality for customer namespaces, such as adding Kubernetes or OpenShift modules, ensuring the functionality has been thoroughly tested and documented before being implemented in a live environment.
- Supported security governance and change management by documenting all live code changes, including tested back-out plans, four-eyes checks, risk assessments, and ensuring strong access management, i.e., escalated privileges on temporary, timed access requests.
- Monitored network activity using Splunk to detect suspicious/abnormal behaviour and take the appropriate action to remediate.
- Committed to knowledge sharing within the quantum cryptography space, including holding presentations to stakeholders.
- Maintained strong knowledge of cyber security frameworks and standards (NIST, ISO 27001).
- Attended regular training on technical skills, such as Terraform and Splunk workshops to ensure cyber security knowledge remained current and up-to-date.
- Adhering to high coding standards, such as the use of white space, meaningful names, readability, and standardised naming conventions.

EDUCATION

SCQF Level 8 in Cyber Security
QA, Edinburgh
Feb 2025