KEVIN GITAU

kevin.gitau27@gmail.com | https://www.linkedin.com/in/kevinkgitau/
Nairobi | +254729648522

Security-focused Technical Support Engineer with over six years of hands-on experience in cloud platform support, vulnerability scanning, access management, incident response, and secure system operations across live production environments. Practical exposure to SIEM concepts, MITRE ATT&CK, container security, and log analysis, backed by certifications in Cisco Ethical Hacking, Google Cybersecurity, and IBM Penetration Testing among others. Comfortable investigating anomalies, supporting secure deployments, performing root cause analysis, and collaborating with engineering and security teams to maintain system resilience and service availability. Brings a structured, detail-oriented approach to incident management and continuous improvement with a genuine passion and a consistent drive to build practical depth.

Work Experience

Technical Support Engineer Dec 2024 - Mar 2026
4RDigital | Remote – U.K

- Executed operational monitoring across Azure-hosted SaaS platforms using Grafana, Prometheus and Application Insights, detecting and resolving availability and performance, anomalies before they impacted users.
- Conducted container security assessments using Trivy and Docker Scout, identifying and remediating Critical and High CVEs across deployment pipelines, while reviewing Azure Front Door and cloud access configurations to strengthen overall security posture.
- Delivered identity and access management improvements by contributing to Entra ID migration activities from Auth0 and validating authentication flows across platform environments.
- Investigated production incidents monthly through SQL queries, log analysis, and API inspection to determine root cause, configuration gaps, and security impact.
- Partnered with engineering teams to remediate findings, validate fixes, and drive down recurrence of platform and security incidents by an estimated 30 percent over the engagement period.
- Automated monitoring, alerting, and reporting workflows using Logic Apps and Power Automate, cutting incident detection and response time by approximately 40 percent.
- Produced runbooks, SOPs, and incident response documentation to standardize troubleshooting and support audit and compliance requirements across the team.

Application Support Analyst Dec 2023 - May 2025
Ateo Finance | Remote – U.S

- Delivered 1st and 2nd Level support for a financial trading platform, resolving 20 plus incidents monthly across application, data, and integration layers in a regulated environment.
- Investigated production issues using log analysis, SQL queries, and data integrity checks, ensuring accurate and secure transaction processing across all platform workflows.
- Monitored scheduled jobs, batch processes, and system alerts across 3 plus environments to identify failures, anomalies, and potential operational or security risks before they escalated.
- Performed root cause analysis on recurring incidents, assessing impact on data integrity, access controls, and system behavior and implementing corrective actions to prevent recurrence.
- Collaborated with internal teams to implement fixes, improve monitoring coverage, and reduce incident recurrence by an estimated 25 percent over the engagement period.
- Authored knowledge base articles, runbooks, and support documentation to standardize response procedures and support audit and compliance needs across the team.
- Supported QA activities for new platform features and bug fixes, validating functionality, edge cases, and regression risks across test and staging environments before changes reached production.

Technical Support Engineer Apr 2022 - Aug 2024
KOKO Networks Limited

- Provided Tier 2 technical support for production IoT platforms, handling 60 to 80 plus tickets per week across incidents and service requests while maintaining SLA compliance throughout.
- Monitored system health, uptime, and alerts across 3000 plus IoT-connected devices using AWS CloudWatch, responding to operational alerts and service degradation events before they impacted field operations.
- Investigated platform and device-related issues using logs, grafana dashboards, and metrics to perform structured root cause analysis, reducing repeat incidents by an estimated 30 percent over time.
- Managed the full incident lifecycle through Jira and Freshservice, maintaining SLA compliance and timely escalations across all open cases at any given time.
- Liaised with development and security teams to escalate bugs, misconfigurations, and access-related issues, ensuring timely remediation and platform stability improvements.
- Supported post-deployment monitoring and validation across releases, ensuring platform stability and catching regressions before they reached end users.
- Queried PostgreSQL databases to validate data integrity, investigate account-specific discrepancies, and confirm correct system states during incident investigations.

Network Operations Center Engineer Sep 2020 - Mar 2022
Adrian Kenya Limited

- Monitored 300 plus customer links via BMC Remedy, maintaining real-time performance tracking and achieving 99 percent SLA adherence across all monitored accounts.
- Escalated and resolved network faults within agreed timeframes, contributing to consistently high customer satisfaction scores across the client base.
- Analyzed network performance metrics using Excel and internal dashboards to identify trends, optimize service delivery, and reduce downtime across monitored environments.

Network Operations Center Engineer Oct 2017 - Jul 2020
Decko Africa LTD

- Delivered first-line support for 30 plus enterprise clients, monitoring network and application dashboards proactively to prevent service disruptions before they impacted customers.
- Escalated incidents in line with ITIL processes, maintaining SLA compliance and clear client communication throughout every resolution cycle.
- Prepared shift handover reports and troubleshooting guides for field engineers, improving incident response efficiency and reducing repeat escalations across the team.

Enterprise systems support Engineer Jun 2014 - Nov 2014
Safaricom PLC - Internship

- Delivered hands-on support for enterprise systems and network services in a live production environment, resolving incidents within agreed SLA timeframes alongside senior engineers.
- Configured and maintained network devices including switches and routers, and executed basic firewall and access control configurations under senior engineer supervision.
- Executed server setup, routine maintenance, patching, and system health checks across Windows and Linux environments, ensuring minimal disruption to enterprise operations.
- Performed system monitoring, log analysis, and fault isolation across managed infrastructure, identifying and escalating root causes of service disruptions before they impacted users.

Core Skills

Monitoring & Observability: Incident response & triage, digital forensics fundamentals, threat intelligence & hunting, MITRE ATT&CK, vulnerability assessment & basic penetration testing, Cisco Ethical Hacking, OWASP ZAP, phishing analysis, email security, endpoint security, SIEM concepts, log analysis, alert investigation
Cloud & Network Security: Azure & GCP security monitoring, identity & access management, Azure AD basics, firewall, VPN, NAC concepts, Cisco ASA/Firepower, Fortinet NSE, IoT & enterprise network monitoring
Data, Scripting & Automation: SQL, PostgreSQL, Python, Bash scripting, reconnaissance, automation, workflow automation, Logic Apps, Power Automate
Monitoring, Platforms & Ticketing: Grafana, Prometheus, Azure Monitor, Application Insights, Jira, Freshservice, Confluence, Slack
Professional Strengths: Root-cause analysis, documentation, Customer support, remote collaboration, SLA-driven operations, AWS CloudWatch, ITIL processes, Auth0, Microsoft Entra ID, Azure Front Door, Trivy, Docker Scout

Education

Jomo Kenyatta University of Agriculture and Technology May 2012 - Nov 2015
Bachelor of Business and Information Technology Information - Second Class Upper Division

Languages

English (Advanced), French (Basic)

Certificates

Certified Ethical Hacker - Cisco

Google Cybersecurity Specialization - Google

Penetration Testing, Incident Response & Forensics - IBM

Foundations of Operationalizing MITRE ATT&CK - AttackIQ

Threat Intelligence Analysis – ArcX

Lateral Connect Cybersecurity Training Program - Lateral Connect

Cloud & Network Security - Cyber Shujaa

Azure Administrator Prep (AZ-104) - Whizlabs

Manage Identities & Governance in Azure - Whizlabs

CCNA (Switching & Routing) - Cisco

Databases & SQL for Data Science - Coursera

Bash & Python Scripting - Coursera / Infosec

IT Service Management Foundations: Tools - LinkedIn