Malik Griffin

Cloud & Security Engineer

Auburn, AL | 678-382-5547 | Malikf83@gmail.com
LinkedIn: linkedin.com/in/malik-griffin-0a13692a6 | GitHub: github.com/malikomari7

Professional Summary

Cloud and Security Engineer with experience designing and supporting hybrid and cloud-native infrastructure with a strong emphasis on security visibility, log correlation, and risk reduction. Skilled in AWS services, automation using Python and PowerShell, API integrations, and containerized workloads. Experienced in IAM governance, network traffic analysis, and infrastructure hardening to improve trust and resilience across cloud and enterprise systems.

Certifications

GIAC GSEC | GIAC GFACT | ISC2 Certified in Cybersecurity (CC) | IBM Agile Explorer | IBM Z/OS Mainframe| AWS SAA (In Progress)

Skills Summary

- Cloud Platforms: AWS (EC2, Lambda, EKS, S3, RDS, SQS, API Gateway), Google Cloud fundamentals
- Application Development: Python, SQL, RESTful APIs, backend service integration
- Containers & Orchestration: Docker fundamentals, Kubernetes (EKS concepts)
- Infrastructure: F5 Load Balancing, VMware, VirtualBox, SAN & storage concepts, UPS and power redundancy
- Networking: VPCs, VLANs, Subnetting, ACLs, VPNs, Cisco Meraki, Aruba, DNS, DHCP
- Security: IAM, MFA, security group design, firewall configuration (Palo Alto, Fortinet)
- Automation & Tooling: Python scripting, PowerShell, PDQ Deploy, Automox
- Operating Systems: Windows Server, Windows 10/11, Linux Ubuntu, MacOS
- Monitoring & Collaboration: Jira, ServiceNow, CrowdStrike, QRadar, DCIM tools

Projects

- F5 Big-IP Log Analysis: Security Data Normalization and F5 BIG-IP Correlation for External to Internal Traffic
- Cloud Application Lab: Built Python-based services integrating AWS Lambda, API Gateway, and S3
- Containerized App Lab: Deployed containerized workloads using Docker and Kubernetes (EKS concepts)
- Secure Home Network Lab: Designed segmented network with firewall rules, VPN access, and monitoring
- Virtualized Infrastructure Lab: Built multi-subnet lab demonstrating DNS, DHCP, NAT, and routing

Professional Experience

IT Infrastructure Analyst — Southern Company (Contract via Synergis)

October 2025 – Present

- Support end-to-end physical infrastructure lifecycle management for enterprise systems, from device request and procurement through delivery, storage, staging, and final installation in the data hall.
- Maintain working knowledge of policies, procedures, and standards governing data center operations, asset handling, and installation workflows.
- Install, cable, and validate enterprise hardware using appropriate fiber and copper media, including single-mode vs. multi-mode fiber, QSFP/SFP optics, and 10Gb/40Gb/100Gb connections.
- Connect infrastructure to firewalls, DMZ environments, SAN storage, and core networking according to approved cable maps, patching plans, and trunking designs.

- Cabling and patching activities to support secure, reliable connectivity while minimizing operational risk.
- Troubleshoot OSI Layer 1 issues following installation, including signal loss, port connectivity, optic mismatches, and cabling faults, in coordination with device owners and engineering teams.
- Participate in capacity and growth planning to ensure adequate rack space, power, cooling, and network connectivity for future system expansion.
- Support a wide range of enterprise and security platforms, including: F5 load balancers, Palo Alto firewalls, Forescout and Corelight security appliances, APCON visibility platforms, Dell SAN and storage systems, Cisco fiber and copper switching, Thales HSM devices
- Manage connectivity between the data center and AP rooms, COAM rooms, and vendor POE rooms, supporting inbound and outbound network paths.
- Assist with early efforts to monitor device alerts and explore API-based integration with asset and monitoring systems for proactive issue detection.
- Use tools such as PuTTY to validate port status and basic connectivity during installation and troubleshooting.
- Coordinate closely with network, security, storage, and system owners to ensure infrastructure is ready for configuration and production use.

IT Systems Technician — Neptune Technology Group
June 2024 – October 2025

- Supported cloud-backed enterprise applications and SaaS platforms for 3,000+ users
- Administered Active Directory and cloud identity services within Microsoft 365
- Troubleshot API-backed authentication flows, VPN access, and wireless network segmentation
- Deployed and automated software delivery using PDQ Deploy, Automox, and Powershell/Python scripting
- Responded to endpoint security alerts and supported access remediation workflows
- Participated in on-call rotation supporting outages impacting cloud and application availability
- Owned and managed service tickets for access provisioning, password resets, and group-based permissions, ensuring prioritization and resolution aligned with established SLAs.
- Provisioned and maintained user accounts and group memberships in Active Directory and Entra ID (Azure AD), applying least-privilege principles and supporting hybrid identity models.
- Administered Microsoft 365 roles, Azure AD app registrations, and certificate renewals, maintaining compliance with enterprise governance and security frameworks.
- Configured and supported Okta SSO integrations, federation protocols (SAML, OIDC), MFA policies, and YubiKey enrollment for enhanced authentication and security.
- Conducted SOX access audits, performed user access reviews, and documented metrics to support regulatory compliance and improve operational transparency.
- Developed and maintained runbook documentation, approval workflows, and metrics dashboards to streamline identity lifecycle operations and support continuous improvement.
- Enabled self-service capabilities for password management and access requests, driving authentication enhancements and supporting troubleshooting across identity layers.
- Investigated and resolved authentication issues involving API-backed flows, VPN access, and wireless segmentation, collaborating with internal teams and service owners.
- Responded to endpoint security alerts, supported access remediation, and maintained awareness of vulnerabilities and breach patterns impacting identity and access systems.
- Led scoped initiatives to optimize provisioning, improve service management processes, and align operational practices with ITIL standards.
- Supported migration activities for virtual machines and firewall systems, ensuring seamless integration and continued security in hybrid environments.
- Mentored Interns and contributed to the development of identity lifecycle standards, promoting best practices and enterprise-wide governance.

Lead IT Field Deployment Technician — MEI, Inc.
January 2020 – August 2022

- Deployed enterprise systems with backend application dependencies in hospital environments
- Installed and configured Windows systems, networking equipment, and segmented VLANs
- Ran and validated fiber optic cabling supporting application and database connectivity
- Integrated UPS systems to ensure up time for computer and application workloads
- Collaborated with vendors including GE Healthcare and Siemens to meet performance requirements
- Installed and integrated advanced clinical systems across imaging modalities including X-ray, CT, MRI, and linear accelerators in enterprise healthcare settings, ensuring seamless interoperability and compliance with hospital standards.
- Performed physical installation, validation, and configuration of vendor solutions (GE Healthcare, Siemens, Varian) using specialized diagnostic tools and adhering to documented deployment protocols.
- Audited and refined deployment workflows to improve system reliability, reduce installation time, and support ongoing process improvement initiatives.
- Configured workstations and wireless access points with segmented VLANs and UPS-backed power to optimize network performance and ensure system uptime.
- Installed operating systems and application software using automated scripting, streamlining setup for clinical applications and reducing manual errors.
- Assisted in device calibration alongside clinical staff and vendor technicians, supporting optimal imaging performance and regulatory compliance.
- Troubleshot connectivity and calibration issues, collaborating closely with hospital IT teams, biomedical engineers, and vendor specialists to deliver timely resolutions.
- Operated in accordance with HIPAA guidelines, maintaining patient data confidentiality and upholding best practices in healthcare IT security.

Education

Bachelor of Science in Computer Science – Cybersecurity (Liberty University | December 2024)