G D Ayegba
Email: tagprime231@gmail.com
Phone: 469-478-1620

Summary

Dedicated Information Security Analyst/Engineer with over 10 years of experience in securing on-premises and cloud environments. Skilled in EDR, SIEM, vulnerability detection/remediation (Tenable.io, Tenable.sc, Qualys, Rapid7), penetration testing (Metasploit, Burp Suite, OWASP ZAP), and incident response. Proven ability to proactively mitigate security risks, ensure data integrity, and align technical security solutions with business objectives. Committed to continuous learning and leveraging the latest technologies to drive organizational security and compliance.

Technical Skills

- Microsoft Azure: Azure DevOps Server, Microsoft Package, Microsoft SSIS, SSAS & SSRS, RStudio, SQL Tools, Putty.
- Operating Systems: Windows Server, Linux distributions (RedHat, Ubuntu, CentOS) - Security hardening and administration.
- Infrastructure & Technologies: Virtualization: VMware ESXi, Microsoft Hyper-V, Citrix XenServer.
- Identity Management: Active Directory, ADFS, Azure Active Directory (Microsoft 365 Hybrid).
- Threat Intelligence: Analysis of threat feeds, vulnerability intelligence (e.g., CVE databases).
- Penetration Testing: Metasploit, Burp Suite, OWASP ZAP.
- Risk Assessment & Management: NIST, ISO 27001, CIS Controls.
- Collaboration & Project Management: Atlassian Suite (Jira, Confluence) and Google Workspace for secure project management, communication, and documentation.
- Cloud Deployment & Management: Secure cloud infrastructure deployment and management using Azure deployment tools.
- Security & Risk Management: Vulnerability Management: Tenable.io, Tenable.sc, Nessus, OpenVAS, Rapid7.
- Data Security: Data Loss Prevention (DLP), encryption technologies (AES, RSA).
- Operating Systems: Windows, Linux and Unix.
- Languages: Java, Python, PowerShell, Prolog, R, C, C#, SQL, BASH scripting.
- Networking Skills: SSL, DNS, DHCP, BGP, TCP/IP, NAT, VPN, ACL. Microsoft Azure, (Azure IaaS, PaaS, VM Migrations, Azure Cloud Services, SQL Azure, Active Directory)

Certification:

Azure Security Engineer Associate
CompTIA Cybersecurity Analyst (CySA+)
Azure Administrator Associate
Azure Solution Architect Expert
CompTIA Security +
CompTIA Network +
Bachelor's in Engineering

Professional Experience

ECG Management Consultant
Senior IT Security Engineer/Security Analyst **October 2022 – Till Date**

- Experienced in Microsoft Security suite such as Microsoft Cloud App Security and MDE. Also, have hands on experience in managing resources in azure portal and azure AD
- Assisted with the implementation of Saviynt Identity Platform, standardizing IAM processes across the organization.
- Leveraged EDR tools such as CrowdStrike Falcon and Microsoft defender for endpoint threat detection and investigation, swiftly identifying and mitigating potential risks.
- Managed enterprise security protocols for a large, multi-tenant network (20,000+ users), implementing secure access policies and troubleshooting remote connectivity issues.
- Conducted regular security audits and application-level vulnerability testing, ensuring system integrity and compliance.
- Performed risk analysis and security code reviews to identify and mitigate vulnerabilities.
- Utilized Tenable.io/SC for network and cloud vulnerability management, prioritizing and remediating identified risks based on CVSS v3 and impact analysis.
- Configured Tenable policies, scanning templates, and asset grouping for targeted vulnerability detection and effective reporting.
- Deployed Tanium to manage patches and endpoint security across the environment, supporting vulnerability remediation and system integrity.
- Administered Pulse Secure SSL VPN for secure remote access, managing clusters to maintain high availability and ensuring compliance with endpoint security policies.
- Configured and optimized advanced VPN security features, including conditional access, multi-factor authentication (MFA), and endpoint checks to safeguard against unauthorized access.
- Executed regular vulnerability assessments using Tenable.io and Tenable.SC, addressing identified risks by deploying patches and system updates to maintain security integrity.
- Provided guidance on identity and access management, leveraging Active Directory and RBAC to manage user permissions across 1,000+ servers and network devices.
- Utilized Tenable.IO for comprehensive vulnerability scanning, device vulnerability assessment, and web application security assessments.
- Conducted detailed vulnerability assessments and penetration testing using Fortify on Demand (SAST), Acunetix (DAST), and Tenable.SC, identifying critical security gaps in cloud and on-premises environments.
- Develop, maintain, and monitor security policies, procedures, standards, and best practices in conjunction with IT leadership, and document your work.
- Architect strategies to protect against, respond to, and recover from security incidents.
- Collaborated on defining and implementing job role and attribute/policy-based access models for enterprise-wide deployment.
- Administered and optimized Azure Active Directory (AAD), including user provisioning, group management, and hybrid identity configurations.
- Configured and enforced role-based access control (RBAC) policies to align with security best practices and compliance requirements.
- Designed and implemented custom Azure group hierarchies, security permissions, and conditional access policies to enhance security posture.

- Integrated AAD with Microsoft Entra ID, third-party applications, and on-prem Active Directory (AD) for seamless single sign-on (SSO) and identity federation.
- Improved organizational security posture by enhancing Microsoft Secure Score through policy updates, identity protection, and multi-factor authentication (MFA) enforcement.
- Implemented Privileged Identity Management (PIM) to enforce just-in-time (JIT) access and minimize exposure of privileged accounts.
- Developed and enforced Zero Trust security models by applying least privilege access controls, password less authentication, and compliance monitoring.
- Develop, implement, and/or maintain tools to assist in the detection, prevention, and analysis of security threats and their impact; manage related vendors, as well as assign help desk tickets.
- Work with the system engineer team on the effective use of firewalls, data encryption, authentication, and other security-related products and features.
- Designed and maintained Azure AD role-based access control (RBAC) strategies to streamline permissions and enhance security compliance.
- Customized user and group permission structures to ensure secure and scalable access management across multi-tenant environments.
- Conducted gap analyses on existing AAD configurations, RBAC assignments, and security policies to identify and mitigate vulnerabilities.
- Provided actionable recommendations for improving security postures, aligning with NIST, CIS benchmarks, and compliance frameworks like FISMA, FedRAMP, and ISO 27001.
- Led security remediation projects, implementing access reviews, log monitoring, and threat detection using Microsoft Sentinel and Defender for Identity.
- Managed and supported Azure Active Directory (Azure AD), including SSO setup, troubleshooting, and user lifecycle management and led operational activities, including access provisioning, de-provisioning, and user lifecycle management for IAM solutions.
- Proactively monitored and responded to security incidents in cloud infrastructure and endpoints, ensuring the protection of organizational assets.
- Collaborated with development teams to identify weaknesses during the software development lifecycle and implemented security-first strategies from design to deployment.
- Developed and maintained incident response plans and procedures, facilitating the timely and efficient handling of security incidents.
- Developed security audits and compliance assessments to ensure regulatory adherence and compliance with industry standards.
- Delivered engaging security awareness training sessions to employees, fostering a culture of cybersecurity awareness and promoting an enhanced security posture throughout the organization.
- Monitored network traffic and analyzed security events using IDS/IPS systems, promptly identifying and investigating potential security incidents.
- Developed custom signatures and rules for IDS/IPS systems, enhancing threat detection capabilities to identify emerging threats effectively.
- Assisted in deploying and configuring firewalls, VPNs, and other network security devices, contributing to the overall network security infrastructure.
- Generated detailed security reports and dashboards to provide improved visibility into security posture and emerging trends.
- Participated in tabletop exercises and simulations to test incident response plans and procedures, ensuring preparedness for real-world security incidents.
- Collaborated with threat intelligence teams to stay abreast of the latest cyber threats and vulnerabilities, incorporating threat intelligence into security strategies.

- Managed identity and access control in hybrid cloud environments, detecting potential misconfigurations or unauthorized access and addressing them by enforcing role-based access controls (RBAC).
- Developed and implemented automated security solutions using Python scripting and APIs, enhancing vulnerability tracking and alerting systems.
- Monitor regulatory and privacy requirements and developments related to security (e.g., HIPAA, GDPR, CCPA), and adjust the security strategy based on these requirements in conjunction with IT leadership.
- Develop and manage the training of the firm's users and IT staff on topics related to information and physical security, cybersecurity, phishing, HIPAA business associate standards, security policies, best practices, etc.

Optimum Technology Inc.
Cloud Cybersecurity Engineer/Identity Engineer **Aug/2019 – October 2022**

- Experienced in Microsoft Security suite such as Microsoft Cloud App Security and MDE. Also, have hands on experience in managing resources in azure portal and azure AD
- Collaborating with application architects and DevOps to modernize our on-premises platform to evolve as infrastructure as a service (IaaS) applications or platform as a service (PaaS); assisting in the administration and governance of Azure Cloud Services
- As senior Engineer, shift focuses to assisting peers any cybersecurity related and technical issues and other sensitive problem.
- Participated in security incident response events, contributing to the organization's proactive security posture and implemented and enhanced user provisioning, deprovisioning, and password management systems for improved security and efficiency.
- Conduct regular account meetings to communicate best practices and future enhancements and develop plans for expanded functionality usage and adoption among client components/chapters.
- Identifying issues related to Vulnerability (CVEs), Compliance (NIST SP 800-190/ PCI/HIPAA/DISA STIG/GDPR/OWASP)
- Responsible for automating incident response workflows by configuring Azure Sentinel Playbooks using Logic Apps, reducing the time to detect and respond to potential breaches and implementing threat intelligence integration to detect and mitigate known vulnerabilities and malicious actors, utilizing third-party threat feeds and custom data connectors.
- Working closely with operational resources to update their on-premises practices and architectures to include cloud service technologies.
- Administered and optimized Azure Active Directory (AAD), including user provisioning, group management, and hybrid identity configurations.
- Configured and enforced role-based access control (RBAC) policies to align with security best practices and compliance requirements.
- Designed and implemented custom Azure group hierarchies, security permissions, and conditional access policies to enhance security posture.
- Integrated AAD with Microsoft Entra ID, third-party applications, and on-prem Active Directory (AD) for seamless single sign-on (SSO) and identity federation.
- Improved organizational security posture by enhancing Microsoft Secure Score through policy updates, identity protection, and multi-factor authentication (MFA) enforcement.
- Conducted security assessments and audits to identify vulnerabilities in identity management, access control, and authentication mechanisms.

- Implemented Privileged Identity Management (PIM) to enforce just-in-time (JIT) access and minimize exposure of privileged accounts.
- Developed and enforced Zero Trust security models by applying least privilege access controls, passwordless authentication, and compliance monitoring.
- Analyzing and identifying applications for cloud assessment and fitment, mapping the workloads across IaaS, SaaS and private clouds and engaging with customer base to understand their evolving business needs and align IT strategy on priorities.
- Experience with Microsoft Intune, Microsoft Defender and 0365 MDM & MAM solutions, Windows autopilot.
- Managed and implemented Azure Sentinel for centralized security event and log management across multiple cloud and on-premises environments.
- Monitored and analyzed security incidents, using Azure Sentinel for real-time detection, correlation, and investigation of potential threats.
- Working closely with Application, Network and Security teams to ensure requirements are reflected appropriately in the Azure-architected design patterns Developing, implementing, and testing data backup and recovery and disaster recovery procedures and writing and maintaining clear, concise documentation; runbooks; and operational standards, including infrastructure diagrams
- Administration of O365 tools; SharePoint, Exchange Online, Teams and OneDrive.
- Design and implementation of ADFS identity solutions for more than Microsoft Office 365. This includes configuring federation trusts with non-Microsoft cloud vendor as well as using ADFS for internal claim aware applications and APIs
- Application deployment in Azure App Service and Application Gateways (WAF and Standard tiers)
- Recommend the establishment or modification of current policies and standards where applicable and assure a good quality of service by providing insight, capacity planning and suitable design
- Cloud Based Migrations: Migrate Exchange to Office Online (O365), Active Directory to Azure Active Directory, workloads, and applications to Microsoft Azure.
- Hub and Spoke network topology architecture for workloads deployment in Azure, Group Policy, Organizational unit configurations and Network and App Security Groups
- Windows Server Configuration and Administration (2012, 2016 2019)
- Database/Application health and performance monitoring experience using services such as OMS and application insight.
- Demonstrated ability to architect and deliver scalable enterprise solutions combining various Azure services.
- Develop and implement IT controls compliance programs that align with SOX and HIPAA regulations. • Provide hands-on technical expertise, guidance, and support for activities including IT SOX Controls, IT HIPAA Controls, IT General Controls, IT Automated Controls and control automation development. • Responsible for the development of new testing automations through the GRC platform, or similar toolsets, to automate the IT internal controls testing (i.e. SOX quarterly controls, data analytics) and the direct gathering
- Experience on PowerShell scripts to automate the Azure cloud system creation including end-to-end infrastructure, VMs, storage, firewall rules.
- Runtime and WAF in customers deployment both on-premises and cloud (AWS / GCP / AZURE/ IBM)
- Demonstrated Experience working with Identity Access Management such as MIM, FIM, MFA, Conditional Access, Azure Information Protection, Device and application management.
- Development of applications using Single Sign-On (SSO), MSAL, or similar authentication libraries, Authentication Protocols and technologies

- Experienced in Federation ADFS, Shibboleth, CA SiteMinder, Okta, PING etc.
- Experienced with security tools such as SIEM, DLP, IDS/IPS, EDR, antimalware, policies, and troubleshooting techniques.
- Experienced in cloud services architecture in engineering technical solutions for Microsoft-centric solutions based on industry standards using Azure specific, hands-on experience with Office 365, Azure policies, Azure Core Platform (Compute, Storage, Networking), Azure Services, Azure AD, Azure Automation, Azure CLI, and PowerShell scripting.
- Demonstrated Experience with ITSM systems, such as ServiceNow and Jira
- Demonstrated expertise with developing strategies for education on and the prevention of spamming, phishing, ransomware, etc.
- Demonstrated expertise with designing and implementing a security infrastructure.
- Demonstrated expertise with Microsoft Azure or other cloud services, Active Directory and Office 365, identity services (e.g AD Connect), infrastructure as a service, server and network virtualization, knowledge of Intune or Group Policy
- Experienced in managing security and infrastructure vendor relationships.
- Strong understanding of and experience with network, server, and application security
- Experience with PowerShell, SQL Server, SharePoint, ServiceNow, Zabbix
- Review documentation such as SSAE 16 or SOC II Reports, along with vendor contracts to ensure that the vendors use best practice and acceptable security measures. Also, organized packages for the Certification and Accreditation of IT systems all controls meet the requirements of NIST using the Risk Management Framework (NIST SP 800-37).
- Developed and customized KQL (Kusto Query Language) queries to create effective workbooks, dashboards, and alerts tailored to the organization's security requirements.
- Integrated Azure Sentinel with Microsoft Defender and other threat intelligence platforms to ensure comprehensive visibility of security events across hybrid infrastructures.
- Solid understanding and experience in cloud computing-based services architecture, technical design and implementations including IaaS, PaaS, and SaaS
- Experienced in system center, Azure Monitoring, Azure Application Insights, Operation Management Suite
- Experienced in Database/Application health and performance monitoring experience using services such as OMS and application insight
- Good Knowledge of networking topologies and engineering, including DNS, Active Directory, Active Directory Federation Services (ADFS), firewalls, load balancers, and gateway devices and Experience with continuous integration (CI)/continuous delivery (CD) models within an agile/Scrum environment a plus
- Work as Cloud Administrator on Microsoft Azure and Azure Virtual Network Management, involved in configuring virtual machines, storage accounts, and resource groups, and also involved with planning, designing, and transforming environments from on-premises to cloud-based
- Writing technical knowledge center articles on architecture and common issues faced by clients.
- Optimize client relationships by building strong and productive relationship with key decision makers
- Nurtures customer relationship and acts as a sales enabler to drive loyalty toward while managing and mitigating risks to the client relationship

Spissys Solutions. **April/2017 – July/2019**
Cloud Engineer/Network Security

- Prioritizing and handling multiple tasks, researching, and analyzing pertinent client, industry, and technical matters, utilizing problem-solving skills, and communicating effectively in written and verbal formats to various audiences (including various levels of management and external clients) in a professional business environment
- Identifying and addressing client needs, building relationships with clients, developing requests for information, demonstrating flexibility in prioritizing, and completing tasks, communicating potential conflicts to a supervisor
  - Provided direction for migration of Windows servers into PCI bubble for compliance
  - Reviewed and Prepared Authorization to Operate Packages (ATO) to meet the guidelines of NIST e.g. (SSP RA, POA&M, CP, PIA E-Authentication and IRP) and ensuring systems go through the steps of the Risk Management Framework.
  - Developed and customized KQL (Kusto Query Language) queries to create effective workbooks, dashboards, and alerts tailored to the organization's security requirements.
  - Integrated Azure Sentinel with Microsoft Defender and other threat intelligence platforms to ensure comprehensive visibility of security events across hybrid infrastructures.
  - Created documentation and path for existing servers to meet PCI standards
  - Directed scans and remediation of servers for PCI certification
  - Experience and familiarity with cloud data security (FISMA/FedRAMP compliance) and working with public cloud solutions (AWS, Google Cloud, and Azure). Comfortable with IaaS, PaaS and SaaS and Worked closely with Engineers to deliver FedRAMP requirements.
  - Experience working with national and international regulatory compliance frameworks such as ISO27000, COBIT, NIST, HIPAA, PCI DSS, and OWASP.
  - Created and documented server hardening policy for new Windows servers
  - Created and documented PCI Procedure Policy for Windows servers
  - Creation and amendment of vulnerability management policy and procedures. Participating in the remediation of Secure Configuration Assessment (SCA) scans, and policy compliance scans (PCI DSS, DISA STIGS, CIS).
  - Initiated PCI scans using Retina Scan tool for Windows servers to assess vulnerabilities.
  - Reviewed current EIQ tool configuration for use in PCI assessment/review.
  - Hardware installation at Disaster Recovery co-location in Aurora, CO as directed.
  - Configured VM networking with reserved IPs, Health Monitors, Firewall rules, VM scale sets, and availability sets in the Azure Cloud.
  - Responsible for end-to-end technical assurance, technical governance, technical best practices, the reuse of technical assets, and the assignment of technical work. Responsible for the technical direction of the project
  - Advanced knowledge of relevant web services, mail, backup, and application monitoring
  - Migrating VDI workload from on-premises to Azure Windows Virtual Desktop along with Windows 10 Multi-session images
  - Provided guidance for a State County on stepwise deployment/migration of SharePoint farm and associated web front ends, proxy servers, ADFS, and SQL database to Azure.
  - Application deployment in Azure App Service and Application Gateways (WAF and Standard tiers)
  - Recommend the establishment or modification of current policies and standards where applicable and assure a good quality of service by providing insight, capacity planning, and suitable design.
  - Reduced process redundancies and learning curves by configuring business rules and transactions to fit each organization’s needs.
  - Responsible for setting and collaborating on cloud vision; providing thought leadership in cloud infrastructure and cloud services architecture to meet operational objectives for cloud solutions.

- Act to resolve issues which prevent effective team working, even during times of change and uncertainty.
- Collaborating and contributing as a team member, understanding personal and team roles, contributing to a positive working environment by building solid relationships with team members, proactively seeking guidance, clarification and feedback.
- Core expertise in S3, Amazon RDS for PostgreSQL, MySQL, MariaDB, Aurora, AWS SFTP, Database Migration Service (DMS), Schema Conversion Tool (SCT) Lambda, VPC, EC2, IAM, KMS and Cloud Formation, Simple Notification Service (SNS), CloudWatch, CloudTrail, KMS.
- Business and Operations Analysis within marketing, operations, or risk analysis using quantitative techniques.

Tx3 Services LLC **Jan/2014 – Mar//2017**

Azure Cloud Engineer

- Experienced in designing cloud, Web, and middleware solutions, supporting them with solution approaches, cloud assessment workshops, POCs, and development/migration Plans.
- Expert with Azure Automation [PowerShell, Azure Resource Manager Templates, Terraform]
- Deployment, administration, and support of company Network infrastructure including WIF network, DMZ, VPN, access points, DNS, and ISP
- On-Premises Platform Migration: Migrate platforms to the latest Microsoft operating systems and Migration Project reviews and guide the team on technical and functional perspectives.
- Support migration of on-premises email and collaboration services to the Microsoft Cloud. This includes having knowledge of Microsoft Identity Manager as well as SQL Server
- Analyzing and identifying applications for cloud assessment and fitment, mapping the workloads across IaaS, SaaS, and private clouds, and engaging with customer base to understand their evolving business needs and align IT strategy on priorities
- Experience with Microsoft Intune: MDM & MAM solutions, Windows autopilot.
- Administration of O365 tools; SharePoint, Exchange Online, Teams, and OneDrive.
- Design and implementation of ADFS identity solutions for more than Microsoft Office 365. This includes configuring federation trusts with non-Microsoft cloud vendors as well as using ADFS for internal claim-aware applications and APIs
- Application deployment in Azure App Service and Application Gateways (WAF and Standard tiers)
- Recommend the establishment or modification of current policies and standards where applicable and assure a good quality of service by providing insight, capacity planning, and suitable design
- Cloud-Based Migrations: Migrate Exchange to Office Online (O365), Active Directory to Azure Active Directory, workloads, and applications to Microsoft Azure.
- Hub and Spoke network topology architecture for workloads deployment in Azure.
- Windows Server Configuration and Administration (2012, 2016 2019)