BOURAIMA DIARRA

bouraimadiarra@protonmail.com | Columbia, MD | 301-957-6891
www.linkedin.com/in/bouraima-diarra | www.github.com/brhymes7 | diarracyberpro.netlify.app

Professional Summary

Dynamic cybersecurity professional with a solid foundation of 5 years in the IT industry, specializing in diverse aspects of cybersecurity and systems management. Currently employed as a Cybersecurity Lead, adept at conducting comprehensive vulnerability assessments, designing intricate architectural diagrams, and streamlining operations through effective automation. My technical proficiency spans System/Network Administration, Software Engineering, and advanced Cybersecurity practices. I am eager to embrace a challenging role that fully utilizes my comprehensive skill set and contributes to innovative solutions in IT security and management.

Education & Certifications

- **CompTIA Security+**
- **CompTIA Network+**
- **B.S. Information Technology**
- **CompTIA CySA+ (In progress)**
- **AZ-500 Security Engineer**
-

Major Accomplishments

- Conducted ASV assessments and presented reports to leadership for PCI-DSS Compliance leveraging PowerBI for data visualization and dashboard building
- Reduced security incidents by 17.5% by implementing secure rules and RBAC within Azure AD
- Structured a robust cybersecurity mesh framework, incorporating Gartner's Zero Trust Architecture (NIST 800-207) with network topology and data flow diagrams
- Migrated an on-premises tenant to Azure with Azure AD Connect and established the Cloud Infrastructure to increase business scalability and efficiency
- Leveraged SCCM (System Center Configuration Manager) within Microsoft Endpoint Manager to deploy, oversee, and maintain applications and services across organizational devices, efficiently handling the distribution of software, updates, and patches.
- Collaborated with the Governance, Risk, and Compliance (GRC) team to assist PCI-DSS Gap Analysis, rendering all documentation of our C1 and C2 assets security
- Constructed a VLAN/WAN hybrid tenant with ADFS (SSO) alongside with Azure resources while implementing least privilege and defense in depth concepts to the entire cloud environment
- Expertly manage GitHub/GitLab repositories and pipelines using Git, facilitating streamlined software development, practicing CI/CD principles, and fostering collaborative project environments.

Compliance & Frameworks

- PCI-DSS
- HIPAA
- TSA
- NIST 800-207
- NIST CSF 2.0
- GDPR
- NIST 800-37
- NIST 800-53
- SOC2

Technical and Non-technical Skills

- Network Security
- Network Segmentation
- Risk Assessments
- Security Auditing
- Cloud Security Architecture
- Incident Response
- Encryption & Data Protection
- Threat Detection & Response
- Vulnerability Assessments
- Vulnerability Patch Management
- Identity & Access Management (IAM)
- Firewalls & Intrusion Detection Systems

Work Experience

IT Security Analyst| Amtrak | Washington D.C | *Full-Time* **Sep 2023 – Present**

- Implemented secure cloud configurations using Azure Private Link, Network Security Groups, Microsoft Defender for Cloud, and Azure Regulatory Compliance for NIST 800-53, PCI DSS, & HIPAA, resulting in 17.5% reduction in security incidents over a year period.
- Automated rollover scans on Tenable by using Python API calls alongside pyTenable library to reduce manual labor hours required for vulnerability assessments.
- Managed Azure cloud services for deploying and scaling web applications, implementing best practices in security and performance to ensure robust digital infrastructure.
- Engineered a Python-based automation tool that integrates data from two Excel files, leveraging the Pandas library for sorting and generating tailored Excel reports for each Point of Contact (POC). Automated the process for data over 100,000 data cells.
- Structured a robust cybersecurity mesh framework, incorporating Gartner's Zero Trust Architecture (aligned with NIST 800-207 ZTA guidelines) to enhance the cybersecurity model with automation and efficiency using LucidChart.
- Constructed Deployment plans for SaaS solutions that were configured and implemented internally within a private Azure Cloud environment.
- Constructed a timesheet app using Microsoft PowerApps, PowerAutomate, Microsoft Lists, and SharePoint to facilitate timesheet process and for metrics visuals with PowerBI.
- Completed Project Lifecycle Management documentation such as Capability Architecture to abide by SAFe procedures and to gain approval from all Digital Technology teams before implementation.
- Supported CI/CD Pipelines within Azure DevOps always ensuring availability.
- Leveraged JIRA and Confluence for project metrics, providing documentation and constructing Standard Operating Procedures to provide stakeholders with insights on progression and completion of tasks.
- Engineered a solution for the ingestion of OT logs into Elasticsearch to build a SIEM dashboard for log analysis and threat detection.

Systems Engineer | Big Thumb LLC, Rockville, MD | *Contract* **Jan 2023 – Sep 2023**

- Migrated an on-premises server to the cloud with Azure VM Service, decrypting LUKS encryption and adding Azure RSA encryption to maximize the security of the resource
- Efficiently resolved technical issues in a high-demand small business environment, utilizing the Web Help Desk ticketing system for prompt and organized response.
- Enrolled and managed devices for the organization across multiple locations ensuring strict compliance with device policy and security standards.
- Automated software and BIOS updates by managing Azure Intune profiles and update rings, streamlining system maintenance and performance.
- Ensured robust network security and compliance with HIPAA and PCI standards by configuring and maintaining M290 firewall, WatchGuard, Barracuda, and Palo Alto systems.
- Delivered expert client assistance remotely via Bomgar, adeptly troubleshooting and rectifying system or network issues to maintain operational continuity.
- Leveraged SCCM (System Center Configuration Manager) within Microsoft Endpoint Manager to deploy, oversee, and maintain applications and services across organizational devices, efficiently handling the distribution of software, updates, and patches.
- Crafted and maintained bespoke PowerShell scripts, significantly enhancing the automation and efficiency of daily administrative tasks.
- Enhanced network performance and security through the implementation and management of Cisco Meraki solutions, optimizing connectivity and monitoring across enterprise networks.

Full Stack Design TA | Rutgers University, Rutgers, NJ | *Part-Time* **Jan 2023 – Sep 2023**

- Simplify and articulate intricate software development concepts effectively, ensuring clarity and comprehension for learners across various skill levels.
- Spearhead the development of a fully responsive React application, employing the MERN stack for robust functionality, Heroku for reliable hosting, and CircleCI to implement Continuous Integration/Continuous Deployment (CI/CD) practices.

Programming Tutor | Tex N Spex LLC, Columbia, MD | *Full-Time* **Jun 2022 – Jan 2023**

- Clarified key concepts in networking and system administration, leveraging tools such as Cisco Packet Tracer, Wireshark, and Nmap, to align their learning with their professional goals.
- Instructed cybersecurity fundamentals using virtual machines, effectively heightening students' awareness and understanding of cyber threats and defenses.
- Established a comprehensive online tutoring infrastructure, integrating e-commerce features to expand and modernize educational services.

Projects/Open Source

Secure Cloud Infrastructure Deployment on Azure | Personal Lab **Sep 2023 – Aug 2024**

- Architected a secure and compliant cloud infrastructure on Microsoft Azure for an e-commerce startup, focusing on security best practices using Azure Virtual Networks (VNet), Azure Active Directory (AAD), and Azure Key Vault.
- Implemented continuous security monitoring through Azure Security Center and Azure Monitor, ensuring real-time tracking of security metrics, detection of vulnerabilities, and compliance with industry standards like PCI-DSS.
- Developed and enforced cloud security policies using Azure Policy and Azure Blueprints, ensuring regulatory compliance and adherence to security best practices across the cloud environment.
- Managed Azure Role-Based Access Control (RBAC) to enforce the principle of least privilege, ensuring that users only had access to the resources necessary for their roles.
- Protected sensitive customer data by utilizing Azure Storage encryption, Azure Disk Encryption, and Azure Private Link, significantly reducing the risk of data breaches and unauthorized access.
- Successfully deployed a secure Azure cloud environment that met regulatory compliance requirements, demonstrating expertise in Azure cloud security, architecture, and regulatory compliance.
- Secured Azure Storage and databases by implementing encryption at rest and in transit, configuring private endpoints, and regularly rotating keys using Azure Key Vault.
- Implemented advanced security controls within Azure, including Network Security Groups (NSGs) and Azure Firewall, to enforce network segmentation and protect against unauthorized access.
- Utilized Azure Bastion to securely manage virtual machines without exposing RDP/SSH to the internet, minimizing the attack surface.

VLAN Network Engineering | Personal Lab **Sep 2018 – Present**

- Scripted commands using PowerShell & Bash to query syslog server and troubleshoot network devices.
- Hosted a responsive webpage store on the VLAN constructed on a LAMP server that enforces RBAC for confidentiality purposes
- Constructed network topology diagram for a Virtual Local Area Network (VLAN) using Cisco Packet Tracer
- Authenticated DNS AD with workstations, Linux syslog servers, and LAMP server using LDAP and Kerberos tools.