# Paul Oriala

(240)-543-2536 | pauloriala@outlook.com | linkedin.com/in/paul-oriala

## Career Overview:

- Over Eight Years of broad-based systems knowledge and management responsibilities covering multiple spectrums of IT
- Focusing on Cyber Security with strong knowledge in information assurance, cyber threat prevention, Cloud Security and SecDevOps

## TECHNICAL SKILLS

**Certifications:** CompTIA Security+ CE | Certified Ethical Hacker | Splunk Fundamentals | Scrum Master | Azure Security Engineer (AZ-500)

**Training:** Microsoft AZ-104 Training | ServiceNow Administration | NIST Cybersecurity Frameworks| RMF Frameworks| NIST-800| ISO 27001| BCP

**Programming Languages:** Python | Java | C++ | PowerShell | Perl | ARM

**Cloud:** Microsoft Azure | Microsoft Azure Gov

**Software & Applications:** Microsoft Office 365 | Service Now |Microsoft SCCM | | Oracle Identity Manager | MS Visual Studio | Confluence

**Network:** Microsoft Active Directory | Wireshark | Citrix VPN | Infoblox | Symantec DigiCert | F5 Network | Barracuda

**Security:** Microsoft Azure IAM | FireEye EX | Splunk SIEM | Malwarebytes | Sentinel One | SailPoint
Varonis | Palo Alto Networks | Dell Cylance | Microsoft Sentinel |Microsoft Defender | Fortinet|
Forgerock | Blackduck | SonarQube | Crowd Strike

**Skills:** Security Audits | ServiceNow Administration | Jenkins | Ansible

**Operating Systems & Databases:** Linux Ubuntu 12 | Windows 10 Enterprise | Microsoft Windows Server 2008/2012 | Microsoft Exchange| IBM Mainframe

## EXPERIENCE

**Volkswagen Automotive Cloud** July 2022 - Current
Lead/Senior Cloud Security Engineer – Contractor 40Hrs/W

- Led Design, Integration, and Deployment of Microsoft Stack for multiple data connectors to create Microsoft Sentinel and Azure Defender functional for the total enterprise environment
- Created and presented findings to Stakeholders, Corporate Leadership, and vendors to display finding and recommend changes that enhanced systems
- Conducted Nist-800-53 Audit assessment for enterprise while also conducting fixes and segmenting work to other teams to conduct fixes.
- Created KQL and Java automation scripts to make security control workflows more efficient, utilized GIT repositories for code review and storage
- Utilized Application security testing tools to automate Static Code analysis, track critically security vulnerabilities and bugs within code
- Managed and maintained the SailPoint platform, including upgrades, patches, and maintenance releases.

**Brown Brothers Harriman** June 2021 – July 2022
Information Security Analyst – Contractor Overnight Shift

- Administered user access controls to prevent unauthorized access during scheduled vulnerability assessments
- Audited departments weekly in compliance with the security baseline within cloud environments and endpoints within Azure Security
- Worked with cross-functional teams to design and implement Identity Governance and Administration (IGA) processes, including role-based access control, user provisioning, and de-provisioning
- Led assigned Attestation Audit reports providing technical competence to Business Presidents & Vice Presidents of Departments
- Utilized IAC to industrialize security infrastructure within Azure & Azure Ad, and its components within the cloud
- Monitored SIEM reporting tools and/or other EDR security tools for alerts, triage alerts, and perform follow-up investigations, focusing on the highest risk alerts first

**WSSC Water**
Computer Systems Analyst / Security Analyst – Contractor December 2020 – May 2022
*Water Company with over 2,000 + employees servicing thousands of clients over the Two Counties*

- Designed, Developed & Implemented software patches for applications and lead the enhancement of 2,000+ systems through

SCCM

- Integrated and updated computer systems with the latest Windows 10 Enterprise version while also adding new functionalities to the existing systems to improve efficiency.
- Managed and configured IBM Mainframe applications for over 2,000+ laptops.
- Conducted System Analysis to ensure proper security posture and effective data protection controls
- Troubleshot and maintained core business applications (Oracle IDM, Oracle MWM, Microsoft O365, Microsoft Licensing)
- Collaborated with the building of Azure Security Controls for onboarding on-prem applications to Azure

**National Science Foundation**

*Tier 3 / Junior Systems Admin – Contractor* June 2020 – November 2020

*Federal Government Agency with 1,700 employees and contractors supporting federal clients*

- Contributed to testing and developing training materials, such as Methods of Procedures (MOPs) and Standard Operating Procedures (SOPs), associated with new products, services, and equipment purposed to create effective workflows.
- Monitored and reported Service-Level Agreements (SLA's) for customers to ensure requirements are met across 2000+ Employees.
- Managed Mailbox databases/ Backups/ Repair/ Recovery through Exchange Server
- Continuously monitored threat data using various analytical methods and Applications such as FireEye and Splunk.
- Scripted AD users and contact object updates using PowerShell to facilitate synchronization to Azure AD
- Part of Cloud Migration project from on-premises servers to Azure

**Fred Accounting & Tax Service**

*Security System Admin* December 2014 – January 2021

- Redesigned and administered ITMS systems, Active Directory, Windows Server, VPN, Microsoft Exchange & SharePoint to increase efficiency and accurate data retention for over 1000+ clients and employees.
- Achieved system updates, disaster recovery plans, SLA agreements, routine QA's, and security logs to maintain proper functionality.
- Performed migration of servers from On-Premises to Azure Cloud, servers from Classic to Azure Resource Manager
- Rendered technical support to resolve issues along infrastructure platforms to sustain 75+ clients weekly.
- Led the proposal, implantation, and integration of advanced efficient frameworks, such as ServiceNow & Microsoft Azure
- Implemented Incident Handling, Hunting, and Malware Analysis, following NIST cyber security framework to secure information and prevent attacks.
- Responsible for Server 2008 installation, configuration and support Active Directory, DNS, DHCP, and WINS, in addition to the migration from Windows Server 2008 to Windows 2016 which advanced system security.

## EDUCATION

**Towson University,** *Fisher College of Science and Mathematics* Towson, Maryland

Major: Computer Science - **Cyber Operations Track**

Minor: Business Administration – **Focus in Leadership & Project Management**

Relevant Coursework: Data Structures & Algorithms, Malware Analysis, Software Security (C++, Java, Python), Network Architecture, Network Security, Operating Systems Security, Application, Software Security, Database Administration

## REFERENCE

Available Upon Request