Derrick Pope | Information Technology Specialist

240-432-7805 | derrick.pope75@gmail.com | Washington D.C. | https://www.linkedin.com/in/derrick-pope/

EXPERIENCE SUMMARY

Amazon Web Services (AWS)
Security Vulnerability Analysis
IAM / SSO / OKTA / SailPoint
OpsBridge Management
Application Performance Manager
AWS Cloud Security

Terraform /Ansible
Data Security/Protection
Bash (Linux)/PowerShell (Win)
Disaster Recovery
Incident Response
Splunk / Tenable / Kenna /Qualys

DataDog /Rapid7/Metasploit
IDS/IPS
Lacework / WireShark
Endpoint Detection and Response (EDR,XDR,MDR)

Results-driven Cloud Engineer with extensive experience securing and automating infrastructure in AWS. Proven ability to architect scalable, highly available, and secure cloud environments using Terraform, Ansible, and AWS-native tools. Skilled in vulnerability remediation, compliance (NIST, HIPAA, ISO 27001), and scripting in Bash, PowerShell, and Python. Successfully led multiple cloud migrations, system hardening initiatives, and DevSecOps implementations within both federal and enterprise environments

TECHNICAL EXPERIENCE & PROJECTS

DATA MIGRATION
- Migrated a large web application's data set from an on-premises MariaDB to AWS RDS, improving performance, durability, and scalability
- Leveraged AWS Systems Manager, Bash scripting, and mysqldump to ensure a reliable and efficient migration process

SERVERLESS APPLICATION DEPLOYMENT
- Develop and deployed a serverless application using AWS Lambda, API Gateway, and DynamoDB
- Implemented serverless functions in Python, enabling scalable and cost-efficient application logic and data processing

HIGHLY AVAILABLE ARCHITECTURE
- Design and implemented a highly available architecture for a critical web application, leveraging services like ELB, ASG, and Multi-AZ
- Ensured maximum uptime and fault tolerance through automated failover mechanisms and proactive monitoring

INFRASTRUCTURE AUTOMATION
- Automate cloud infrastructure provisioning and management using Terraform and Ansible
- Defined reusable IaC templates for EC2, ALB, RDS, IAM roles, and security groups to streamline deployments across dev/test/prod environments
- Integrated user-data scripts and SSM commands for seamless server bootstrapping and patch automation.

RESILIENT CLOUD ARCHITECTURE
- Designed and deployed a highly available architecture using VPC**,** Auto Scaling Groups**,** Application Load Balance**r**, and Multi-AZ EC2 deployments
- Implemented custom AMIs, automated scaling policies, and health-based failover using CloudWatch Alarms and target groups
- Deployed a static website using S3 + CloudFront with security hardening (block public access, origin access identity, HTTPS enforcement).

CLOUD SECURITY ASSESSMENT
- Perform cloud security assessments by utilizing security assessment tools , Pacu, Scout Suite, Prowler.
- Manage cloud vulnerability remediation using AWS Security Hub, Inspector, and other cloud security tools.
- Configured and installed server-based certificates ensuring best practices and meeting compliance requirements

SECURITY ASSESSMENT
- Conduct comprehensive security assessments of IT systems and applications, identifying vulnerabilities, weaknesses, and compliance gaps using Qualys and Splunk.
- Facilitated tabletop exercises to simulate real-world security incidents and test the organization's incident response

procedures and capabilities.

WORK EXPERIENCE

Aug 2023 – Present

Information Technology Specialist * U.S Dept. of Treasury 5000 Ellin RD, Lanham MD 20706 * 40 Hours per week * Richard Patterson (901)214-2999

- Lead and manage security strategy, ensuring alignment with NIST 800-53, ISO-27001, and HIPAA frameworks.
- Conduct all risk assessments and vulnerability scans; coordinate mitigation plans directly with application owners and stakeholders
- Oversee critical updates and patching for OBM (Ops Bridge Manager) organization application monitoring service and APM (Application Performance Manager), ensuring uptime and compliance.
- Implement software updates and vulnerabilities using Linux and PowerShell commands, ensuring secure and up to date systems
- Installed server-side certificates to ensure compliance requirements and NIST 800-53 best practice.
- Implement and maintain high-level technical documentation to support repeatable and auditable security operations.
- Ensure strict operational security during system updates and infrastructure changes, reducing downtime by 15%.
- Execute audits using Splunk, Qualys, and vulnerability management platforms, maintaining system integrity and compliance posture.
- Perform security audits on application agents for verifying their security, accuracy, and compliance with organizational policies, ensuring data integrity and preventing vulnerabilities.
- Coordinate and manage team own application documentation for Federal Information Security Management Act (FISMA) Master Inventory database.
- Manage and validate Entity History Log (EHL) file used by Customer Account Data Engine (CADE) 2, CADE2 is an IRS system designed to modernize and improve the processing of taxpayer accounts
- Lead the department's Risk-Based Decision (RBD) process and compliance reviews for major systems.
- Developed comprehensive documentation for the update process to enhance future operational reference and minimize errors
- Coordinate weekly security meetings with application owners and vendors for remediation solutions ensuring best practices.
- Solely responsible for reviewing, developing, and maintaining security policies, plans of action, and milestones (POA&Ms).
- Manage and configure downtime requests using the organization's monitoring tool (Ops Bridge Manager **–** OBM), ensuring alert suppression during scheduled maintenance windows

Sep 2020 – Mar 2023

DevSec Engineer * United Health Group 3000 K St NW Washington D.C. 20007 * 40 Hours per week * Charles Black (858)999-5347

- Managed and responded to security alerts from tools like Data Dog and PagerDuty, optimizing configurations and developing response documentation for the Security Operations Center.
- Deployed and utilized Carbon Black Endpoint Detection and Response (EDR) for continuous monitoring, threat detection, and response for endpoints, which leverages behavioral analytics and machine learning to identify and respond to advanced threats detection, deployed agent on over 200 devices.
- Performed security analysis in AWS accounts to detect suspicious activities using security tools, CloudTrail, Athena queries.
- Reduced risk by ensuring coverage of malware detection for in-scope Carbon Black EDR Agent capable devices.
- Provided follow-up reports (technical findings, feedback, resolution steps taken) for Root Cause analysis, engineering technical assessment and process improvement initiatives
- Conducted threat analysis, achieving 99% data security and mitigating all risks in a 24/7 environment.
- Implemented security measures such as creating security Slack channels for threat detections and providing subject matter expertise in security reviews.
- Identified and neutralized over 250 viruses and hidden malware using Tenable/AWS Inspector, preventing exploitation on 78 servers
- Updated security policies and plans following industry standards (NIST-800.53, ISO-27001, HIPAA) and implemented CIS Benchmark recommendations.
- Automated system deployment with Terraform, managed vulnerability alerts with Kenna/AWS Inspector, and performed threat modelling and risk assessments.

- Managed software updates and vulnerabilities using Linux and PowerShell commands, ensuring secure and up to date systems.
- Developed and maintain documentation for security systems and procedures.
- Developed and documented Disaster Recovery and Business Impact Analysis (BIA) plans, ensuring business continuity and recovery procedures.
- Stayed updated on the latest security trends, technologies, and threats to continuously enhance security posture.

Jul 2018 – Sep 2020

Security Specialist * Rally Health 3000 K St NW Washington, DC 20007 * 40 Hours Per Week * Carla Wheeler (847) 502-3589

.

- Performed security assessment on security systems to strengthen security posture for the organization.
- Created Active Directory accounts for over 500 users and computer management
- Worked closely with senior engineers, other team members and application owners to solve technical problems at the network, system and application levels
- Utilized Tenable for scanning and testing to identify potential targets.
- Conducted security risk assessments, identifying vulnerabilities and recommending remediation measures.
- Developed and implemented security policies and procedures to ensure compliance with industry standards and regulations were in compliance with NIST RMF, ISO 27001, PCI, HIPPA frameworks and regulations
- Led incident response efforts, investigating security breaches, and implementing corrective actions.
- Collaborated with cross-functional teams to design and deploy security infrastructure, including firewalls, intrusion detection systems, and access controls.
- Participated in security audits and compliance assessments, addressing findings and implementing necessary controls.
- Managed vulnerability database (ManageEngine) to collect, maintain and review data about discovered computer security vulnerabilities.
- Identified vulnerabilities on networks and servers using ManageEngine.
- Utilized basic digital forensics techniques with Wireshark.
- Implemented Compliance and Assessment procedures using Cybersecurity Maturity Model (CMM).

Jan 2018 – Feb 2022

Security Analyst * UrbanEd Academy 2041 Martin Luther King JR Ave SE Washington D.C. * 30 Hours Per Week * Roxanne Williams(202) 610-2344

- Led security assessments and vulnerability scanning to identify and mitigate risks, adhering to standards such as HIPAA, ISO/IEC 27001, and NIST 800-171
- Performed vulnerability scans on network hosts using Metasploit
- Utilized Rapid7 for vulnerability remediations
- Installed and configured computers and peripherals in a Windows 11 enterprise environment

- Monitored security systems, promptly responding to potential security incidents and alarms
- Implemented threat and vulnerability management concepts to ensure a secure environment
- Identified and remediated vulnerabilities on networks and servers, enhancing overall security
- Deployed and utilized vulnerability scanning tools like Wireshark, Nmap, and Nessus

Jun 2006 – Feb 2018

Security Advisor * American Society of Clinical Oncology 2318 Mill Road Alexandria, VA 22314 * 37.5 Hours Per Week * Tabari Layne(202)468-5930

- Assisted in conducting risk assessments and vulnerability scanning to identify and mitigate security risks.
- Monitored security systems and promptly responded to security incidents and alarms.
- Collaborated with IT teams to implement security controls and ensure secure configuration of systems and networks.
- Created documentation for emergency preparedness plans.
- Conducted periodic security audits and assessments to evaluate compliance with industry standards and policies.
- Managed the coordination of new hire orientation onboarding and exit notification procedures.

EDUCATION

UrbanEd Academy

University of the District of Columbia

CERTIFICATIONS

CompTIA Security+ | CompTIA A+ Technician

CISSP Certified Information Systems Security Professional (expected completion June2025)

240-432-7805 | derrick.pope75@gmail.com | Washington D.C., 20005