RONNIE BAILEY

Richmond, Virginia // Tel: (360) 719-8377
ronniebailey@live.com // linkedin.com/in/ronniebailey

Expert in cloud security and access management with 10+ years of experience. Skilled in implementing cybersecurity solutions, ensuring compliance, and leading strategic projects to enhance operational security and efficiency.

TECHNICAL PROFICIENCIES

ADVANCED NETWORK SECURITY & ACCESS SOLUTIONS:

- BeyondTrust, Cisco Meraki, Citrix, Fortinet Suite, Ping Identity, SSL/TLS Management, vSphere, Webex

CLOUD IDENTITY & SECURITY SERVICES:

- AWS, Azure AD/Entra ID, Google Portal, SiteMinder

COMPLIANCE & SECURITY FRAMEWORKS:

- Business Continuity Planning, Data Classification, Disaster Recovery, FISMA, HIPAA, HITRUST, ISO 27001, NIST

CYBERSECURITY OPERATIONS & TOOLS:

- Confluence, CrowdStrike, Microsoft 365, MFA, Rapid7, RSA, Security Identity Manager, ServiceNow, Varonis

DEVOPS & SECURITY AUTOMATION:

- Agile, API Management (Apigee, Auth0), Digital Asset Mgmt, GitHub, JavaScript, JSON, PowerShell, Python, REST API, Scrum, Waterfall

ENTERPRISE IDENTITY & ACCESS MANAGEMENT:

- Access Control / Change Management, Active Directory/GPO Administration, Access & Identity Management, CyberArk, Directory Services, ForgeRock, Identity Solutions Design & Implementation, Microsoft Intune (MDM), OAuth, OIDC, OneIdentity Safeguard: Privileged Passwords, SAML, SSO, Saviynt IGA, Total Privileged Access Management (TPAM)

IT INFRASTRUCTURE & OPERATIONS MANAGEMENT:

- Infrastructure & Service Management, Linux Mainframe, Windows Server

THREAT DETECTION & VULNERABILITY MANAGEMENT:

- IBM QRadar, Kali Linux, McAfee Enterprise Security Manager, Security Information Event Management (SIEM), Splunk

CAREER

IDENTITY AND ACCESS MANAGEMENT (IAM), ARCHITECT

Kroger, Technology & Digital Department 12/2022 - Present

- Enhances organizational security posture and compliance, leveraging Microsoft Azure for cloud services and OneIdentity Safeguard and TPAM for identity and access management, ensuring scalable and secure cloud infrastructure managing cybersecurity policies ensuring the compliance of 500,000 employee profiles.
- Reduces system vulnerabilities and improves threat detection and response through the integration of CrowdStrike, focusing on advanced endpoint security.
- Drives the adoption of SailPoint, resulting in a 45% improvement in audit performance and a 35% reduction in unauthorized access through refined identity governance and automated provisioning processes.
- Streamlines user access control and identity management with Active Directory and LDAP, facilitating secure and efficient authentication processes.
- Integrates Okta to provide seamless identity and access management across cloud and on-premise applications, reinforcing the security framework.
- Protects sensitive information and ensures regulatory compliance by employing Varonis for data security analytics.
- Supports secure collaboration and information sharing using Confluence, SharePoint, and Microsoft 365, incorporating security measures into business operations.
- Manages and secures privileged passwords with One Identity's Privileged Password Management (PPM), addressing access-related vulnerabilities.
- Oversees security projects and initiatives, utilizing Jira for effective tracking and execution, ensuring timely completion of security priorities.

SR. PRINCIPAL SECURITY ARCHITECT

Department of Homeland Security, United States Secret Service 2/2022 - 12/2022

- DHS Public Trust Clearance active until June 2025.
- Streamlined CyberArk's Privileged Access Management system, boosting audit compliance by 50% and cutting response times by 40% through implementing advanced security protocols and integrating automated threat detection features.
- Orchestrated cloud migration using Azure AD, ensuring secure and efficient transfer of critical systems from on-prem to cloud environments.
- Utilized Agile development and scripting languages (PowerShell, Python) for system resilience and efficiency in accordance with the FISMA framework.
- Designed and implemented identity solutions using Active Directory, OAuth, and SAML, emphasizing cloud security.
- Managed the Department of Homeland Security & Secret Service enterprise network security program, promoting IAM governance and utilizing scripting knowledge.
- Monitored server and firewall logs, analyzed network traffic, and conducted regular vulnerability scans using tools like Qualys to maintain robust security.

SR. PRIVILEGE ACCESS MANAGEMENT (PAM), ENGINEER

Lands' End 12/2021 - 12/2022

- Deployed OneIdentity Safeguard for robust privileged password management, integrating it with existing systems for streamlined access control.
- Designed, implemented, supported, and maintained the PingIdentity SSO platform,OpenID Connect, OAuth 2.0, and MFA.
- Conducted regular audits and adjustments of privileged access settings, leveraging OneIdentity's analytics to enhance system security.
- Directed enterprise migration to Azure AD, achieving a 40% improvement in login efficiency and halving identity-related incidents by leveraging SSO and integrating with existing infrastructure.
- Provided end-to-end support for the Identity and Access Management lifecycle, including on/off-boarding, conversions, transfers, IAM compliance, and role management.
- Experienced in security protocols such as LDAP-S, SAML, WS-Federation, SCIM, OAuth, and OIDC.
- Evaluated existing security technologies and recommended the adoption of new and emerging IAM solutions, such as Auth0, to enhance the organization's security posture.
- Effectively communicated critical updates to key stakeholders throughout the organization, utilizing collaboration tools like Confluence.

INFOSEC ADMINISTRATOR

Accessia Health 7/2021 - 12/2021

- Managed vulnerability assessments, remediation strategies, and ensured HIPAA and NIST compliance.
- Enforced SP 1800-30 guidelines to protect confidential data in healthcare applications and general Internet access.
- Implemented CrowdStrike Falcon, increasing threat detection by 95% and minimizing incident response time, utilizing AI-based analysis and automated response capabilities.
- Conducted system audits and policy enforcement for robust security compliance.
- Regularly updated security protocols in alignment with the latest QRadar documentation, ensuring optimal configuration for threat detection.
- Maintained server compliance with the ACF2 environment through Unix scripting.
- Ensured continuous functioning of system interfaces/connectors, coordinated with IT.
- Implemented Auth0 for secure, scalable user authentication, leading to a 99% success rate in logins and halving the development time for new auth features by leveraging customizable workflows and SDKs aligning with HIPPA requirements..
- Developed a centralized incident response management system on GitHub, facilitating team collaboration on playbooks, real-time incident tracking, and knowledge sharing on threats. This approach streamlined response times by 30% and enhanced team efficiency in threat resolution.

IDENTITY AND ACCESS MANAGEMENT (IAM), PRINCIPAL ENGINEER

Indivior Pharmaceuticals 10/2019 - 7/2021

- Integrated SSO and MFA using Microsoft Azure Active Directory, enhancing user verification processes and access management.
- Ensured ePHI data protection and encryption through off-site backups and Bitlocker.
- Designed IAM solutions using Microsoft Intune for efficient mobile device management, ensuring secure and remote access.
- Managed user account profiles in Active Directory and Linux Server for access control and security.
- Led the deployment of BeyondTrust to secure privileged accounts, reducing unauthorized access by 75% and enhancing compliance by 80% through strategic account management and audit controls.

IDENTITY AND ACCESS MANAGEMENT (IAM), ANALYST

Wells Fargo 4/2019 - 10/2019

- Ensured IAM practices were compliant with the bank's operational risk framework and industry best practices, including policies, procedures, and control methodologies.
- Managed and configured user roles and permissions in Active Directory, utilizing GPOs for enforcing security policies across the network.
- Established and maintained user accounts, profiles, network and system security, and access privileges through IAM tools such as Active Directory, Office 365, and SCCM.
- Supported IAM solutions design and maintenance, focusing on access control systems.
- Conducted on and off-boarding and trained 400 employees on security processes, reducing phishing attacks.
- Upgraded email security with Proofpoint, reducing phishing attempts by 60% and malware incidents by 45% through advanced threat protection and targeted attack analysis.

CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM) ENGINEER

Wellsecured IT 10/2015 - 1/2019

- Orchestrated the migration of legacy IAM systems to ForgeRock IDM, improving identity lifecycle management and reducing operational costs.
- Integrated Splunk with IAM solutions to automate the collection and analysis of access logs, streamlining audit processes and significantly improving the efficiency of compliance reporting.
- Provided complex technical guidance, oversight, and enforcement of security directives, policies, standards, plans, and procedures as defined by ISO/IEC 27001 framework.
- Conducted comprehensive security audits using Ping Identity tools to identify and remediate potential vulnerabilities in the IAM infrastructure, aligning with best practices and compliance standards.

- Installed virtual machines (VMWare, VirtualBox, & Hyper-V) to utilize applications in a test environment.
- Designed and deployed a suite of PowerShell scripts for automating security tasks, including log analysis, system hardening, and incident detection. This initiative reduced manual security analysis time by 50% and improved threat detection speed by 40%.
- Integrated Auth0 for scalable user authentication, enhancing authentication success to 99% and cutting development time by 50% by adopting secure and efficient authentication workflows.

CLOUD SECURITY OPERATIONS

Cloudcentria Security 6/2011 - 12/2015

- Developed and maintained policies, procedures, and documentation to align with regulatory standards, leading to successful audits and certifications.
- Designed role-based, location-based, & device compliance access controls for Entra ID.
- Developed custom Splunk searches and alerts to proactively identify and mitigate potential security breaches within the IAM framework, ensuring compliance with industry standards and regulatory requirements.
- Led the integration of Ping Identity with enterprise applications, ensuring secure and efficient user access control to reduce administrative overhead.
- Upgraded email security with Proofpoint, reducing phishing attempts by 60% and malware incidents by 45% through advanced threat protection and targeted attack analysis.
- Maintained high-level customer satisfaction by delivering professional and timely support, and documenting processes and service desk records meticulously.
- Created industry leading practices of Identity and Access Management/Access Control/Change Management through Active Directory and Azure AD PaaS.

EDUCATION

- **Bachelor of Science in Cybersecurity,** University of Richmond (6/2024)
- **Associate of Applied Science in Information Systems**, Reynolds College (5/2021)

CERTIFICATIONS

- **AZ-900**: Microsoft Azure Fundamentals (In progress)
- **Cybersecurity Essentials,** Cisco Networking Academy
- **Network Administration,** Reynolds College

AWARDS AND HONORS

- Phi Theta Kappa Honor Society, international honor society
- President's List, Reynolds College