RONNIE BAILEY

RICHMOND, VA | (360) 719-8377
career@ronniebailey.cloud | linkedin.com/in/ronniebailey

ABOUT ME

Senior Cloud Security professional with over 10 years of industrial experience implementing integrations, tests, operations, migrations, and maintenance of cloud-based security solutions that meet operational and security compliance requirements for stakeholders.

EXPERIENCE

- Access Control/Change Management
- Active Directory/GPO Administration
- Amazon Web Service
- API Management/Apigee
- Auth0
- Azure AD
- Bomgar/BeyondTrust
- Cisco Meraki
- Citrix Remote Desktop
- Confluence
- Crowdstrike
- Data Classification
- Documentation
- Fortinet suite
- HIPAA, NIST frameworks
- HRIS/ UltiPro/ Workday
- Hybrid Migration, On-Prem to Cloud
- Identity Solutions Design & Implementation
- ISO/ NERC CIP/ NIST/ SEC 501
- Linux Mainframe Environment
- Microsoft 365
- Microsoft Intune
- Mobile Device Management (MDM)
- OAuth, OIDC, SAML, SSO
- OneIdentity Safeguard
- Password Management
- PingFederate
- Powershell Scripting
- Python
- Rapid7
- REST API/ JSON/ JavaScript
- RSA MFA
- SAML, OAuth, OIDC, SSO
- ServiceNow
- Varonis
- Windows Server Administration 2012/2016/2019

CAREER

IDENTITY & ACCESS MANAGEMENT, ARCHITECT SME

3/2022 – PRESENT | D.H.S., U.S. SECRET SERVICE

- Performs IAM architect duties in the development, design, and implementation of IAM solutions with a process driven focus allowing the ability to leverage against the right tool for the right use case.
- Designs and deploys Cloud Identity Management solutions, identity workflows, and drives auditing and compliance initiatives utilizing Zero Trust methodologies to reduce organizational risk appetite and attack the surface.
- Develops meaningful enterprise security metrics, leveraging enterprise knowledge to demonstrate effective risk management and to build security capability and maturity.

- Improves IAM system architecture including SSO Federation using SAML, OIDC/OAuth 2.0, and Kerberos authentication standards.
- Provides leadership and mentors a team of cyber security professionals to provide an extremely high level of availability and end user satisfaction which results in onboarding and access requests
  efficiency being raised by 73% across the organization.
- Assists with influencing the information security risk direction of others to drive corporate risk acceptance to successful completion within the technology risk standards and guidance.
- Advises and collaborates with IT and business leaders to develop and implement layered security controls for protecting the privacy, confidentiality, integrity and availability of client information, corporate data and networks.
- Integrates automation that improves service delivery to the agency by reducing the time to make changes and the risk of making errors.
- Manages DHS enterprise network security program for 23,000 customers.
- Promotes IAM governance including role-based access control, access request, and certification.
- Leverages scripting knowledge to execute automation within Powershell.
- Performs IT consultations for defining, designing, implementing, supporting, and overseeing client information security infrastructure to determine proper scalable solutions based on individual business requirements.
- Monitors, tracks, and records system performance and utilization metrics.
- Documents and thoroughly understands IAM applications architecture, system configuration across platforms, and interface with various systems, and uses this knowledge effectively to resolve potential issues.
- Leading project lifting IT governance framework from on-prem to on-cloud environment.
- Generates roadmaps and participates in the standards process for IAM solutions, establishing procedures for user access to the system, setting access controls, and administrative practices.

IDENTITY & ACCESS MANAGEMENT SOLUTIONS ENGINEER
6/2011 – PRESENT | CLOUDCENTRIA SECURITY

- Leads and coaches' direct team and cross-team members on security best practices.
- Partners with security, enterprise, technical and application architects to champion secure by design principles and help deliver secure and reliable solutions that challenge status-quo while modernizing the IAM practice, platforms and services.
- Directed, coordinated, implemented, executed and controlled services ensuring consistency with business direction and compliance with Cloudcentria standards, policies, procedures, and management to established budgets.
- Built strategic relationships with delivery partners and vendors to establish an adequately diversified supply chain that is efficient, resilient, and responsive to changes in business demand.
- Communicated the companywide architecture strategy and direction to both management and systems related teams.
- Supported the Identity and Access Management group within information and cybersecurity, providing strategic and architecture guidance and collaborating with teams on design and implementation projects.

- Supported information security technologies in different domains with a focus on identity and access management solutions and controls including: application and database security, cloud, network and infrastructure security, and cryptographic algorithms and key management.
- Provided artifact creation in the form of position papers, blueprints, patterns, and reference architectures.
- Lead architectural support for product and vendor evaluations for solutions intended to address IAM functionality while addressing relevant security threats.
- Provided oversight and technical leadership across all cybersecurity functional domains to ensure confidentiality, integrity, and availability of all systems.

SR. CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM) ENGINEER
12/2021 – 12/2022 | LANDS' END

- Exerted expert knowledge of implementing SAML, OpenID Connect (OIDC), OAuth 2.0, SSO, identity gateways and MFA.
- Articulated cybersecurity architecture vision, security strategies and risk implications to key stakeholders to guide leadership decision-making.
- Led implementation expertise with LDAP, PKI, Mobile MFA, OTP, and mobile security through Azure AD/AWS/GCP cloud platforms as well as on prem.
- Applied robust knowledge of Identity and Access Management providing end-to-end lifecycle support from HR driven processes, including on/off-boarding, conversions, transfers, IAM compliance, and role management.
- Provided understanding and hands-on experience with Ping Suite of products such as PingFederate, PingAccess, PingDirectory, and PingOne for customers.
- Documented experience with designing, implementing, supporting, and maintaining of PingIdentity SSO platform.
- Managed domain object lifecycles (joiners, movers, leavers) through automation and integration with key systems through Ping, UltiPro, and Powershell.
- Monitored the system's interfaces/connectors to ensure they were always functioning.
- Led the collection and analysis of business and technical requirements to develop retail center IAM processes and procedures.
- Created IT and business documentation for controls to standardize internal processes and procedures for Changed Management/Access Control and Privilege Access Management (PAM).
- Effectively communicated highly technical information to both technical and non-technical personnel.
- Experienced in leading workshops/discussions with customer, customer team(s) and vendor team(s) for issues, platform enchantment, design etc.
- Participated in software development in following programming languages, Java, SQL, and JavaScript.
- Experienced in security protocols such as LDAP-S, SAML, WS-Federation, SCIM, OAuth, and OIDC.
- Conducted knowledge of all procedures, standards, and regulations for authorization and Authentication.

SECURITY NETWORK ENGINEER
7/2021 – 12/2021 | ACCESSIA HEALTH

- Monitored, evaluated, and maintained systems administration and procedures established to safeguard information assets from intentional or inadvertent access or destruction through AD policy enforcement and governance utilizing security frameworks of NIST and HIPAA.
- Coached team on company policies, compliance, procedures, and best practices to enhance operational efficiency, employee productivity and subsequently decrease labor costs meeting SOP's.
- Monitored the system's interfaces/connectors to ensure they are always functioning.
- Coordinated with IT on issues requiring technical or interface support.
- Documented and enforced SP 1800-30 guidelines ensuring confidential data was protected to healthcare. applications as well as general Internet access for patients and visitors using Cisco Meraki.
- Installed and maintained security products including firewalls & Identity Access Management (IAM.)
- Collaborated on multiple hybrid-based assignments, simultaneously, in a fast-paced environment.
- Utilized Python scripts to push and pull data between databases and the target LDAP directory.
- Maintained server compliance with the mainframe ACF2 environment by running scripts in Unix via Putty.
- Leveraged platforms driving compliance throughout security integrated AD for 500 user accounts.
- Led critical cloud security platform initiatives including synchronization with Microsoft Bitlocker.
- Exported account/group/role data, created and deleted accounts and group/role memberships.

IDENTITY AND ACCESS MANAGEMENT ADMINISTRATOR
10/2019 – 7/2021 | INDIVIOR PHARMACEUTICALS

- Ensured all ePHI data was protected and encrypted by supervising off-site backups of electronic files and maintained an audit trail to make documentation so that patient information is kept safe while in storage and transit by using Microsoft Bitlocker.
- Investigated threats, managed policy for Host Based Security System (HBSS) using Ivanti, performed asset discovery, compliance scans using Microsoft Intune, Azure AD Services, and Defender.
- Managed user account profiles in Active Directory and Exchange Server for password resets, account unlocks, and security access to firm based applications and services.
- Configured and authenticated Microsoft Defender for Exchange and Office 365 email experience.
- Administered Identity and Access Management in a hybrid environment to decrease the inherent risk related to identity governance, using an API tool to feed back and forth from AD to cloud environments.

- Managed and conducted a site wide inventory project for 200 laptop computers, mobile devices, and user licensed applications quarterly, following ITIL best practices.
- Designed and presented end-user support documentation and training to promote IT security compliance while increasing adoption rates of newly deployed products and services. Define and document best practices and support procedures.
- Utilized Fortinet tools to ensure company compliance via NIST-800 framework for endpoint security.
- Administered security and end user management across a mature IT environment of various types of endpoints including Linux, Mac, and Windows through RBAC in Active Directory.

IDENTITY & ACCESS MANAGEMENT TECHNICAL OPERATIONS SR. ANALYST
4/2019 – 10/2019 | WELLS FARGO

- Ensured IAM practices were compliant with the bank's Integrated Operational Risk Framework and industry best practices as it relates to: Policies and procedures Level 1 and Level 2 control methodologies for a permanent control framework that align business coordination with different bank compliance and internal control streams LOB entities and unit level compliance and operations control assessments.
- Designed plans for the future strategy of internal facing systems and infrastructure including Windows 10 migration projects, Azure AD migrations, and Mobile Device Management solutions.
- Identified internet services issues through root cause analysis, supported trouble tickets submitted directly with software such as ServiceNow and hardware vendors.
- Scheduled follow ups regarding tickets to offer complete 93% of resolutions within projected SLA's.
- Established and maintained user accounts, profiles, OS upgrades, endpoint/server patching, access privileges and overall network and system security through IAM tools: Active Directory administration and governance, Office 365 Administration, Exchange Server, SCCM, SAML, PING, ForgeRock, and SailPoint IdentityNow.
- Conducted on and off-boarding, in addition to training 400 employees on security processes and risk mitigation techniques in the organization reducing phishing attacks.
- Analyzed and implemented systems to deliver comprehensive development life cycle solutions.
- Worked with event management and ticketing tools to monitor for preventative maintenance, improving IT department's effectiveness by 35% with the use of SCCM tools.
- Managed phishing simulation campaigns to test compliance while offering ongoing training and remediation on best practices of IPsec.
- Provided essential system and network administration support for servers, network hardware, data storage equipment, printers, workstations and other network connected hardware and associated software.
- Worked closely with software and hardware vendors to accurately document changes in processes for troubleshooting and remediation.

IDENTITY AND ACCESS MANAGEMENT ANALYST
10/2015 – 1/2019 | WELLSECURED IT

- Created and maintained documentation of the IT Risk program and any exceptions for regulatory compliance.
- Effectively utilized the proper resources to develop solutions and devise new approaches to tasks related to maintaining secure transmission of sensitive organizational data.
- Performed implementation, upgrade and testing tasks for systems and network security technologies through utilization of change control methodologies.
- Engaged in the guidance and advisement of less experienced systems security analysts.
- Installed virtual machines (VMWare, VirtualBox, & Hyper-V) to utilize applications in a test environment.
- Created industry leading practices of Identity and Access Management/Access Control/Change Management through Active Directory and Azure AD PaaS.
- Provided complex technical guidance, oversight, and enforcement of security directives, policies, standards, plans, and procedures as defined by ISO/IEC 27001 framework.
- Defined and documented IT security requirements and communicated through effective security programs and training.
- Provided technical and administrative support in the modification, design, and set-up of applications security.
- Evaluated and resolved security related problems and advised users on security issues.
- Compiled and documented data in support of equipment and/or user changes of system migrations.

EDUCATION

BACHELOR OF SCIENCE IN CYBERSECURITY,
5/2023 | UNIVERSITY OF RICHMOND | RICHMOND, VA

ASSOCIATE OF APPLIED SCIENCE IN INFORMATION SYSTEMS,
8/2020 | REYNOLDS COLLEGE | RICHMOND, VA

CERTIFICATION

AZ-900, MICROSOFT AZURE,
3/2023 | IN PROGRESS

CYBERSECURITY ESSENTIALS,
10/2021 | CISCO NETWORKING ACADEMY

NETWORK ADMINISTRATION,
8/2021 | REYNOLDS COLLEGE