

RAGA RISHITHA DUTTA

Systems Engineer | Cloud Security | Identity & Access Management | Zero Trust

rishithadutta5@gmail.com | +1 (856) 526-2032 | LinkedIn: <https://www.linkedin.com/in/rishithadutta/>

OPEN TO RELOCATE

PROFESSIONAL SUMMARY

Systems Engineer and AI Systems Integrator with 3+ years of experience across enterprise identity and access management, cloud security, AI-enabled systems, Zero Trust, infrastructure, security operations, and technical support. Skilled in Okta, Microsoft Entra ID, AWS, Azure, CyberArk, SailPoint, Terraform, Splunk, CrowdStrike, Zscaler, ServiceNow, PowerShell, and Python. Experienced in IAM administration, access governance, privileged access management, cloud security, automation, incident triage, systems integration, troubleshooting, and compliance-focused change management across regulated environments.

CORE SKILLS

Identity & Access Management: Okta, Microsoft Entra ID, Active Directory, SailPoint IdentityIQ, Ping Identity, SSO, MFA, RBAC, Conditional Access, Access Reviews

Privileged Access Management: CyberArk, Credential Vaulting, Session Monitoring, Just-in-Time Access, Privileged Account Governance

Cloud & Infrastructure Security: AWS IAM, Azure RBAC, Azure Security, Terraform, Infrastructure as Code, Cloud Security Posture Management

AI Systems Integration: AI System Integration, AI-Enabled Security, AI Risk Management, Anomaly Detection, API/Endpoint Integration, Python Automation

Zero Trust & Network Security: Zscaler, Zero Trust Network Access, Microsegmentation, Least Privilege, NIST SP 800-207

Security Operations: Splunk, SIEM, EDR, CrowdStrike, Detection Rule Tuning, Alert Triage, Incident Response Support, Security Monitoring

IT Operations & Support: ServiceNow, Windows Server, Microsoft 365, Group Policy, Troubleshooting, Incident Management, ITIL, SLA Management

Compliance & Governance: SOX, PCI DSS, Access Certification, Change Management, Security Controls, Audit Support

Scripting & Tools: PowerShell, Python, Git, Jupyter Notebook, ServiceNow

PROFESSIONAL EXPERIENCE

Truist Bank, Charlotte, NC August 2025 – Present

Systems Engineer

- Administer enterprise Identity and Access Management using Okta and Microsoft Entra ID, supporting Single Sign-On, Multi-Factor Authentication, Conditional Access, and identity lifecycle management for 10,000+ users across on-premises and cloud environments.
- Apply Zero Trust security principles across network and application layers, enforcing least-privilege access and continuous identity verification aligned with NIST SP 800-207.
- Manage privileged access workflows in CyberArk, including credential vaulting, session monitoring, and Just-in-Time access provisioning, reducing standing privileged access by 40%.
- Automate cloud identity and access policy enforcement across AWS and Azure using Terraform and native Role-Based Access Controls.
- Configure and tune Splunk SIEM detection rules for identity-based threats including impossible travel and privilege escalation; support security operations teams with alert triage and incident response.
- Support identity governance programs using SailPoint IdentityIQ, including access certification campaigns, RBAC modeling, entitlement reviews, and compliance controls for SOX-regulated banking environments.
- Partner with network security teams to deploy Zscaler Zero Trust Network Access, modernizing remote access and replacing legacy VPN connectivity.
- Document, track, and coordinate infrastructure and security changes through ServiceNow and Change Advisory Board processes.
- Evaluate AI-based anomaly detection capabilities in Splunk to identify unusual identity and access behavior and improve security alert fidelity.

Technical Environment: Okta, Microsoft Entra ID, CyberArk, SailPoint IdentityIQ, AWS IAM, Azure RBAC, Terraform, Zscaler, Splunk, CrowdStrike, ServiceNow, PowerShell, Python, NIST SP 800-207

Sports Media Inc, United States November 2024 – July 2025

AI Systems Integrator

- Integrated AI-enabled systems and cloud services with enterprise identity, access control, and security requirements, supporting secure authentication and authorization workflows.
- Designed and implemented IAM integrations for AI systems using Microsoft Azure and AWS, including Single Sign-On, Multi-Factor Authentication, Role-Based Access Control, and least-privilege access.
- Developed and tested secure access workflows for AI model endpoints, training data, model outputs, and supporting cloud resources.
- Applied Zero Trust architecture principles and identity governance concepts to AI system integration, emphasizing continuous verification, least privilege, and controlled access.
- Built Python automation and testing scripts to validate authentication, authorization, API/service integrations, and security controls within AI-enabled environments.
- Integrated and evaluated security monitoring and AI-driven anomaly detection capabilities to identify unusual access behavior and support incident triage.
- Reviewed NIST SP 800-207 and AI security/risk management practices to inform secure AI system design and access-control decisions.

- Created technical documentation, integration procedures, test results, and presentations for cross-functional stakeholders.

Technical Environment: Azure, AWS, Microsoft Entra ID/Azure AD, Python, IAM, Zero Trust, AI Systems Integration, RBAC, SSO, MFA, NIST SP 800-207, Git, Jupyter Notebook

Jarus Technologies, Hyderabad, India September 2022 – June 2024

Junior System Administrator | Client: Penn National Insurance

- Supported senior systems engineers with IT infrastructure, identity management, end-user support, and access administration for a U.S.-based insurance client in a remote delivery model.
- Created and managed user accounts, groups, Group Policy, and access permissions in Active Directory for 500+ employee accounts across business units.
- Supported employee onboarding and offboarding, including provisioning and deprovisioning access to applications, email, shared resources, and enterprise systems.
- Monitored, triaged, and resolved incidents and service requests through ServiceNow, maintaining 95% SLA compliance for response and resolution.
- Provided technical support for password resets, Multi-Factor Authentication setup, access issues, and account troubleshooting.
- Assisted with Windows server and workstation patch management, system updates, maintenance scheduling, and operational documentation.
- Created standard operating procedures for recurring IT support and access-management activities to improve consistency and team efficiency.
- Participated in client status meetings and reported ticket volume, resolution metrics, SLA performance, and ongoing support activities.

Technical Environment: Active Directory, Windows Server, Group Policy, ServiceNow, MFA, Microsoft 365, Networking Fundamentals, ITIL Processes, End-User Support

EDUCATION

Montclair State University, Montclair, NJ — MS in Cybersecurity

St. Martin's Engineering College, Hyderabad, India — B.E. Computer Science and Engineering