

ALEX MERELUS

+1(678) 725-5553 ✉ alexmerelus@gmail.com 🌐 www.alexmerelus.me 🔗 www.linkedin.com/in/alexmerelus/

SUMMARY

As an Identity Access Management Administrator I specialize in safeguarding critical IT infrastructures by ensuring the integrity and security of access controls. With a comprehensive understanding of identity and access management (IAM) principles, I am committed to implementing and optimizing identity governance strategies. My experience encompasses program development, policy enforcement, risk mitigation, and compliance adherence within a dynamic and evolving cybersecurity landscape. I utilize tools such as SailPoint IdentityNow, ServiceNow, and Jira to achieve these goals. I thrive in collaborative environments, working alongside cross-functional teams to maintain a secure and compliant organizational ecosystem.

EDUCATION

WESTERN GOVERNORS UNIVERSITY

Salt Lake City, UT

M.S. in Cybersecurity and Information Assurance

OAKWOOD UNIVERSITY

Huntsville, AL

B.S. in Business Finance

EXPERIENCE

Inspire Brands

Orlando, FL

Identity Access Management Engineer

Nov 2023 - Present

- Successfully integrated IAM policies and procedures, focusing on adherence of access certifications for SOX standards using SailPoint IdentityNow, Active Directory and Workday.
- Reviewed controls and control evidence, contributing to the organization's overall security assurance by ensuring adherence to regulatory standards and preparing for control assessments, resulting in improved audit readiness.
- Utilized ServiceNow for effective ticket management and auditing of access controls, as well as maintaining an SLA in line with industry standards.
- Handle Web Automation Testing with API tools such as Postman to manage SailPoint IdentityNow Access Requests and ensure proper Site functionality.
- Developed a reporting system to analyze identity accounts and manage any uncorrelated and inactive to reduce attack surface and vulnerabilities.
- Collaborated on the development of a security automation roadmap, outlining automation initiatives to enhance process efficiency, reduce manual intervention in security tasks, and achieve a 20% reduction in manual security operations for the upcoming year.
- Leveraged Agile methodologies to deploy and streamline Role-Based Access Control (RBAC) solutions, enhancing and revamping the identity management infrastructure for improved security and efficiency.

DxFeed/DevExperts

Jersey City, NJ

Information Security Specialist

March 2022 – Nov 2023

- Orchestrated secure cloud configurations across AWS platforms using Nessus: Boosted system integrity and reduced vulnerabilities by 60% over six months, improving security posture for mission-critical systems.
- Championed SOC-2 compliance Initiatives by taking an active role in the execution of compliance strategies, placing a significant emphasis on identity lifecycle management and best practices for access control.
- Participated in SIFMA's annual Business Continuity (BC) and Disaster Recovery Plan (DR) testing: Reinforcing the organization's commitment to data protection and resilience.
- Enhanced collaboration using Agile tools like Atlassian Jira with internal and external technical teams to ensure robust and secure data handling.
- Reviewed vulnerability management findings and contributed to the governance of the CSIRT operating model, ensuring alignment with best practices for incident response and mitigation, resulting in a 15% reduction in response time for critical incidents.

Eretmis

New York, NY

PCI DSS Consultant

Nov 2022 – May 2023

- Evaluated Internal IT Controls: Conducted comprehensive system assessments, enhancing alignment with PCI DSS standards, leading to a heightened security profile and reduced vulnerabilities.
- Led Network Audits: Collaborated closely with cross-functional teams, overseeing detailed audits and compliance questionnaires, ensuring robust and secure critical information systems.

- Promoted IGA Principles: Crafted and provided actionable security recommendations, driving a marked improvement in organizational security and compliance standards.

Apple, Inc
Technical Security Expert
 March 2022

New York, NY
 May 2020 –

- Maintained adherence to Apple's security protocols to consistently uphold industry regulations and ensure the security of customer data and privacy.
- Executed identity governance strategies, significantly reducing potential breaches and safeguarding sensitive customer user data, and introduced identity protection techniques, countering threats and mitigating potential vulnerabilities.
- Spearheaded compliance and remediation processes, collaborating with cross-functional teams, and ensuring a strict alignment with industry standards and cybersecurity best practices.
- Deployed endpoint security on user devices using advanced tools, emphasizing data loss prevention and access management. This resulted in effectively countering vulnerabilities, leading to a 30% reduction in security incidents.

Apple, Inc
Technical Specialist

New York, NY
 Oct 2019 – May 2020

- Mitigated mobile device risks by deploying comprehensive risk mitigation techniques, enhancing user data protection against sophisticated threat actors.
- Developed and conducted meticulous monthly security sessions, tailoring content to address pressing issues, thereby elevating the organization's security posture.
- Optimized security remediation protocols, enhancing threat resolution efficiency during periods of heightened security alerts, resulting in a 25% improvement in incident response time
- Educated users on mobile device management best practices, ensuring secure device deployment for employees and enhancing overall security posture through advanced features.

Apple, Inc
Apple-Care Support Advisor

New York, NY
 May 2015 – Oct 2019

- Coached 34 colleagues over six-month periods on key technical tools and concepts, enhancing team proficiency and elevating customer support quality.
- Enhanced endpoint security by utilizing anti-malware tools, successfully resolving and removing over 1,000 vulnerabilities regularly, and ensuring a consistently secure baseline configuration.
- Guided customers through technical troubleshooting and resolved complex issues across Apple products, enhancing customer trust and brand loyalty. Tailoring communication strategies for diverse audiences and collaborated with cross-functional teams, boosting resolution efficiency and customer satisfaction.
- Leveraged customer interactions to provide feedback for product enhancements, simultaneously balancing multiple support tasks and engaging in continuous learning sessions to maintain up-to-date product knowledge.

PROJECTS

Azure Vulnerability Remediation (Home Lab) – www.github.com/alexmerelus/Azure-SOC

- Designed and deployed a Cloud Honeynet within Microsoft Azure as an integrated Security Operations Center (SOC) to proactively identify threats, simulate attack scenarios, and enhance cybersecurity infrastructure.
- Conducted in-depth security analysis and incident response adhering to the NIST 800-61 Incident Management Lifecycle.
- Managed cybersecurity operations by monitoring traffic and access attempts through Network Security Groups (NSGs), ensuring secure data flow between Azure AD (Microsoft Entra ID), SQL Databases, and Virtual Machines.
- Leveraged Azure Log Analytics Workspace for logging and real-time analysis of honeynet activity, and utilized Microsoft Azure Sentinel for advanced threat detection, alerting, incident visualization, and threat modeling, ensuring proactive identification of potential threats.
- Evaluated and fortified the cybersecurity posture before and after applying security control measures in line with NIST 800-53 (SC-7: Boundary Protection) and utilized Azure Microsoft Sentinel for SIEM operations, resulting in a strategic improvement of early threat detection and SOC monitoring capabilities.

Azure AD RBAC Automation (Home Lab) – www.github.com/alexmerelus/Azure-AD-RBAC-Automation

- Developed and deployed a Python automation script that streamlined 100% of secure role assignments in Microsoft Entra ID (Azure AD), reducing manual role configuration by 90%.
- Created a custom Azure-style log generator that produced over 500+ security event logs, including unauthorized access attempts and login success/failure patterns for Splunk ingestion.

- Designed and implemented 2 Splunk dashboards visualizing 100% of ingested security data, improving visibility into security events and enabling real-time monitoring for unauthorized access attempts.
- Documented compliance mapping & policy development for 4 compliance frameworks (NIST 800-53, ISO 27001, SOC 2, CIS Controls v8) with 100% alignment to project reports and dashboards, ensuring adherence to best practices for IAM lifecycle management and data retention.
- Created 3 incident reports covering Unauthorized Access Analysis, Frequent Resource Changes, and Login Success vs. Failure to align with industry standards, supporting 100% traceability of security incidents.
- Utilized 5+ technologies including Python, Azure SDK, Splunk, Key Vault, Faker, enhancing data simulation and security monitoring for IAM governance.
- Published a 100% complete project structure on GitHub, including a refined README, 4 policy and compliance files, and a compliance mapping document, improving project clarity and professionalism.

CERTIFICATIONS, PUBLICATIONS, and CPEs

- | | |
|--|--|
| • CompTIA – Security + | • Google - Cybersecurity Professional Certification |
| • CompTIA – CySA + | • Microsoft (SC-900) - Security, Compliance, and Identity Fundamentals |
| • CompTIA – PenTest + | • Qualys Certified Specialist - PCI Compliance |
| • (ISC) ² CC - Certified in Cybersecurity | • SailPoint IdentityNow Security Leader |

SKILLS AND TOOLS

GitHub, Qualys Guard, Vulnerability Management, NIST controls, Wireshark, AttackIQ - Foundations of Operationalizing MITRE ATT&CK, AWS Security Fundamentals, Microsoft Azure, Nessus, Business Continuity, IT Security, OWASP TOP 10, ServiceNow, Microsoft PowerPoint, Excel, Teams, Outlook, SailPoint IdentityNow, Postman, Atlassian Jira, Confluence, SOAR Implementation, Application Threat Modeling, Security Automation Roadmap Development, Security Assurance.