18 Arthur Ave, Barrie, Canada
jijojoseph1993@gmail.com
+1 (431) 726 2369

Jijo John Joseph

Security-focused professional with over 5 years of hands-on experience in Mobile Device Management, particularly with Workspace ONE, complemented by a good background in Data Analytics and Cybersecurity. Known for seamlessly integrating cutting-edge technologies and methodologies to streamline operations and enhance security measures.

Education

Big Data Analytics

Georgian College, Barrie, ON – Canada

May 2023 — December 2023

- Graduated with honour, achieving an overall percentage of 92.29%.

Information System Security (Cyber Security)

Georgian College, Barrie, ON - Canada

May 2022 — April 2023

- Graduated with honour, achieving an overall percentage of 90.33%.

Bachelor of Technology

Mohandas College of Engineering and Technology, Trivandrum, Kerala – India

August 2012 — April 2016

- Graduated B.Tech, majored in Computer Science and Engineering with First Class.

Work Experience

Ministry of Public and Business Service Delivery, Guelph, ON - Canada

January 2023 — April 2023

Field Service Agent (Co-Op Student)

- Directed mitigation efforts for IT security incidents involving compromised passwords and phishing schemes, leading cross-functional teams in incident response and recovery procedures, cybersecurity resilience and reduced breach impact by 50%.
- Report and document security incidents to Level 2 team for investigation.
- Executed responses to tier 1 customer queries over the phone, honing customer service competencies and bolstering technical support proficiency by 60%.
- Practiced and improve problems based on determination skills to quickly dissects technical problems as described by non-technical people improving turnaround time by 80% for tickets.

- Expedited technical support to government employees to address hardware, software, OS, and hand-held device issues either in person or via remote technology.

Allianz Technology SE, Trivandrum, Kerala - India September 2016 — April 2022

Senior Technical Analyst

- Established and configured Organization Groups within Workspace One UEM-MDM from inception, ensuring seamless functionality and alignment with organizational goals.
- Configured and deployed applications to mobile devices, encompassing both internal and public applications for iOS and Android platforms for 60,000 device fleet.
- Served as a Subject Matter Expert for iOS, macOS, and Android platforms, providing valuable insights and guidance to enhance operations.
- Enforced security best practices and protocols to safeguard sensitive data and ensure regulatory compliance across all devices and platforms.
- Integrated Lookout for enhanced mobile threat management and response capabilities, ensuring comprehensive security coverage for 30,000 mobile devices to ensure compliance and security.
- Implemented robust security measures such as Data Loss Prevention (DLP) for both mobile and macOS platforms, including encryption protocols, access controls, and device compliance policies.
- Ensured regular security audits and assessments to identify vulnerabilities and mitigate risks.
- Orchestrated patch management and automated notification for updates using Workspace One Intelligence, bolstering system resilience and security.

Projects

Service Now Integration with Workspace One

Integrated Workspace One UEM with Service Now for end-to-end ordering using Workspace One API with the help of orchestrator which has the functionalities Account creation, Device registration, Device Deletion and Account Deletion ensuring an automated ordering process.

macOS Management with Workspace One UEM

Developed and implemented Workspace ONE UEM for macOS (COBO- Corporate Owned, Business Only) operating model, integrating Apple Business Manager and enabling seamless AD user activation with User Approved and DEP following information security guidelines by CISO that includes DLP policies and standards.

Lookout Integration with Workspace ONE UEM

- Integrated the application 'Lookout' with Workspace One for Mobile Security, Phishing, and identity protection for close to 35,000 mobile devices by using API Administrators and setting up Lookout tenants.
- Created compliance policies and tags associated with each risk and application status.

Android Enterprise with Workspace One UEM

Lead the development of Android Enterprise with work Profile and COPE (Corporate-owned Personally enabled) devices (7000 Android devices) using Workspace One along with application deployment and enforcing security policies for data protection.

AWS Infrastructure Cloud Migration

Key player in the smooth cloud migration of 60,000 mobile devices from on-premise to AWS Cloud platform by creating component testing plans, reporting bugs, facilitate and plan seamless S/MIME certificate delivery without services interruption.

Technical Skills

- HTML & CSS
- Azure Active Directory
- Workspace One
- Wireshark
- Tableau
- Apache Spark and Hive
- Jira
- Monitoring and Log analysis
- Microsoft SQL (SSMS)
- Python
- Microsoft Intune
- SIEM- Splunk Enterprise Security
- Lookout Mobile Endpoint Security
- Microsoft Office
- GitHub
- Microsoft Power Automate
- Application Programming Interfaces (API)
- Identity Access Management
- Metasploit
- Rapid Miner
- Public Key Infrastructure (PKI)
- Windows, macOS and iOS

Non-Technical Skills

- Team skill
- Self-Learner
- Root Cause Analysis and problem solving
- ITIL
- Documentation
- Flexibility
- Agile Methodologies
- Risk Assessment and Mitigation
- Communication skill

Licenses & certifications

- SAS Visual Analytics 1 for SAS Viya: Basics, SAS
- DASA DevOps Fundamentals, APMG International
- ITIL V4 Foundation