Sushanth Kummari

Systems Engineer III

9951479193
sushanth3048@gmail.com
LinkedIn

OBJECTIVE

Experienced Identity and Access Management (IAM) professional with strong expertise in **CyberArk Privileged Access Management, PKI certificate management, and Active Directory / Azure Active Directory (Entra ID)**. Proven experience in automating privileged account onboarding, certificate renewal, and BigFix patch management across on-prem and AWS EC2 environments. Skilled in designing end-to-end automation workflows using **PowerShell and Python**, improving security, compliance, and operational efficiency. Adept at implementing least-privilege access, maintaining audit-ready environments, and collaborating with cross-functional teams to enhance enterprise security posture.

PROFESSIONAL EXPERIENCE

FactSet – Systems Engineer III

Duration: May 2023 – Present

- Managed end-to-end daily operations of CyberArk Privileged Access Management (PAM), including onboarding and offboarding of privileged accounts, access approvals, password rotation, reconciliation, and decommissioning across enterprise environments.
- Built basic AI-driven automations to interact with users, triage issues, answer common queries, and route cases to the appropriate support teams.
- Engineered CI/CD automation using GitHub Actions to orchestrate Windows patching, application upgrades, and operational workflows across distributed environments.
- Led the end-to-end deployment of a new Active Directory domain, including designing the domain architecture, promoting and configuring the first Domain Controller (DC), DNS integration, and baseline security hardening.
- Implemented a self-hosted CyberArk PAM platform from scratch **[Lab]**, including vault setup, core component installation (PVWA, CPM, PSM), initial configuration, security hardening, and onboarding of target systems and privileged accounts.
- Troubleshoot CyberArk password failures, reconciliation issues, and login/authentication errors to ensure uninterrupted PAM operations in Production and UAT environments.
- Performed automated password rotations for local and service accounts on target hosts within CyberArk Production, ensuring compliance with security policies.
- Collaborated with vendors and internal teams during CyberArk Vault migration activities across UAT and Production environments, ensuring data integrity and minimal downtime.
- Remediated security vulnerabilities identified on CyberArk infrastructure, strengthening the overall PAM platform security posture.
- Participated in End-of-Life (EOL) activities for CyberArk servers, ensuring secure decommissioning, credential cleanup, and data protection.
- Supported CyberArk SOX compliance reviews and audit readiness initiatives by providing evidence, access reports, and configuration documentation.
- Automated IAM, PAM operations, compliance checks, and patching workflows using PowerShell and Python, significantly reducing manual effort and operational risk.
- Executed and monitored BigFix patch management activities, including patch deployment, validation, and compliance reporting, to meet internal security and regulatory standards.
- Performed regular access reviews and compliance audits across CyberArk, Active Directory, Azure Active Directory, and AWS environments.
- Collaborated with cross-functional stakeholders to design, implement, and enforce identity and access security frameworks across Windows Server, Active Directory, and Azure AD platforms.
- Administered Active Directory services, including user and group management, service accounts, Group Policy Objects (GPOs), replication, DFSR, and authentication protocols.
- Supported Azure Active Directory (Entra ID) operations, including hybrid identity management, role-based access control (RBAC), and secure authentication policies.
- Managed AWS IAM users, roles, and policies to secure cloud workloads and enforce access governance.
- Administered PKI infrastructure using Venafi, managing certificate lifecycle operations such as discovery, renewal, expiration monitoring, and cryptographic compliance.

- Maintained comprehensive documentation for PAM configurations, IAM processes, automation scripts, and operational procedures to support audits and knowledge transfer.

R1 RCM – Systems Engineer
Duration: April 2023 – May 2023

- Managed Active Directory and Azure Active Directory (Entra ID) environments, overseeing user access lifecycle, authentication mechanisms, group policies, and security controls to ensure seamless and secure identity management.
- Developed and enhanced PowerShell automation scripts to streamline administrative and IAM operational tasks, improving efficiency, accuracy, and response times.
- Built strong expertise in IT infrastructure fundamentals, including networking concepts, cloud services, and security best practices, to support optimized system performance and secure identity integrations.

TeamWare Solutions (Microsoft) – Technical Support Engineer
Duration: Jan 2022 – Feb 2023

- Assessed, optimized, and enhanced IT infrastructure security, performance, and operational efficiency across enterprise environments.
- Installed, configured, and troubleshoot software, hardware, and Windows Domain Controllers, ensuring high availability and system stability.
- Administered Active Directory services, including DNS, domain and forest architecture, trusts, replication, and performance optimization.
- Diagnosed and resolved authentication and authorization issues involving NTLM, Kerberos, and frequent account lockouts.
- Created, configured, and troubleshot Group Policy Objects (GPOs) and Fine-Grained Password Policies (FGPPs) to enforce security standards.
- Upgraded forest and domain functional levels and performed Domain Controller promotion and demotion activities.
- Resolved Active Directory replication failures, trust relationship issues, and performed stale object and metadata cleanup.
- Implemented Local Administrator Password Solution (LAPS) to secure local administrator accounts and configured Kerberos delegation (2-hop authentication).
- Diagnosed and remediated slow logon issues, user profile problems, and cross-site Active Directory replication delays.
- Provided technical knowledge sharing, incident triaging, root cause analysis, and maintained comprehensive operational documentation.

JD Sports – Systems Administrator
Duration: Oct 2021 – Jan 2022

- Installed, configured, and troubleshot server-class systems, hardware, and software to ensure optimal performance, stability, and availability of IT infrastructure.
- Administered Active Directory and Microsoft Exchange environments, managing user accounts, groups, policies, and enterprise email services.
- Streamlined system onboarding and offboarding processes through SCCM-based imaging, deployment, and configuration management.
- Provided technical support and troubleshooting for authentication and logon issues, application failures, VPN connectivity, and end-user access problems.
- Maintained standard operating procedures (SOPs), technical documentation, and knowledge base articles to improve operational efficiency and support continuity.

Pyramind IT (Wipro) – Support Engineer
Duration: Apr 2020 – Oct 2021

- Provided end-user technical support for Windows operating systems and Microsoft Office applications, ensuring a smooth and productive user experience.
- Assisted in the installation, configuration, and maintenance of SCCM infrastructure to support reliable system deployment and performance.
- Installed, configured, and optimized network cabling, hardware, and software components to improve overall network efficiency and system stability.
- Managed helpdesk operations by diagnosing and resolving hardware, software, and connectivity issues, ensuring timely incident resolution.
- Performed regular server backup operations and system maintenance activities to prevent data loss and ensure high system reliability.

- Conducted user training and provided assistance on software updates, system enhancements, and basic troubleshooting best practices.
- Handled service requests and incidents within defined SLA timelines, ensuring uninterrupted IT operations and high user satisfaction.

KEY PROJECTS

Automated CyberArk PAM Bulk Onboarding

CyberArk PAM | Safes | Platforms | Policies | PowerShell

- Automated bulk onboarding of privileged accounts into CyberArk PAM.
- Created Safes, assigned platforms, and applied policy configurations using plugins.
- Reduced onboarding time and ensured consistent PAM security controls.

PKI Certificate Auto-Renewal & Deployment

PKI | Venafi | PowerShell | Email Automation

- Monitored SSL/TLS certificates and triggered renewal before 20 days of expiry.
- Automated certificate deployment to websites with minimal downtime.
- Implemented email alerts for success, failure, and expiry notifications.

Automated BigFix Patching – AWS EC2

AWS EC2 | BigFix | Patch Management | Automation

- Discovered EC2 instances from onboarded AWS accounts and installed BigFix client.
- Implemented full automation flow: Maintenance Mode → VIP → Patch → Validation.
- Installed software during Maintenance Mode to ensure zero production impact.

End-to-End Patch Orchestration – On-Prem Servers

BigFix | Windows Server | PowerShell

- Automated patching workflow with pre and post-patch validations.
- Enabled Maintenance Mode and VIP handling to avoid service disruption.
- Improved patch compliance and reduced manual effort.

EDUCATION

University of Hyderabad – Post Graduate Diploma in Project Management
Passout Year: 2021

CMR Institute of Technology – BTech in Electonics and Computer Engineering
Passout Year: 2019

GMR Polytechnic Gajwel – Diploma in Electonics and Computer Engineering
Passout Year: 2016

TECHNICAL SKILLS

CyberArk PAM (Vault, PVWA, CPM, PSM, CP/CCP, Safe Management, LDAP, PTA, AIM)	AI Automation (Basic) – Automated user interaction, issue triage, FAQ handling, and support ticket creation/escalation.	PKI / Venafi (Certificate Lifecycle, Renewal, Compliance)	Identity & Access Management (Azure AD, AAD Connect, GPO, LAPS, IAM Lifecycle, Access Controls)	Active Directory & Windows Server (2012 R2–2022, DFSR, Authentication, SSO Integration, GPOs)
Infrastructure & Security (SQL, Web Servers, OS Troubleshooting, Security Hardening)	Cloud & Automation (Azure, AWS, PowerShell, Python, REST APIs, HTML)	Privileged Account Automation (Onboarding, Offboarding, Rotation)	Monitoring & Auditing (Splunk, Grafana, System Audits)	Patch Management (BigFix, Compliance Reporting)
ITSM & Process (ServiceNow, Remedy, ITIL, Incident & Change Management)				

SOFT SKILLS

Security Mindset	Proactive & Innovative Thinking	Problem Solving & Root Cause Analysis	Automation & Process Optimization	Incident & Crisis Management
Team Collaboration &	Exploratory & Continuous	Documentation,		

Stakeholder Management Learning Compliance & Audits