MANIK SINGH BANDRAL

📞 +91 9906102726 ✉ hiremaniksingh@gmail.com 🏠 Trikuta Nager, Jammu, J&K, India

SUMMARY

Highly motivated IT Infrastructure and Monitoring Analyst with almost 3 years of experience in IT infrastructure, cloud platforms, and security monitoring. Skilled in GCP, Microsoft 365, Azure AD, and network security. Expertise in Microsoft 365, Intune, Azure AD, network security & troubleshooting, incident response & security alert monitoring, PCI DSS & ISO 27001 compliance, and SSL certificate management. Adept at handling Level 1 and Level 2 IT support, ensuring optimal system performance and security. Strong knowledge of firewall management (SonicWall and Meraki) and IT Security & governance. Proven ability to work with cross-functional teams to deliver high-impact IT solutions.

EDUCATION

Bachelor's in Computer Application (BCA)
Bachelor's Degree in Computer Application
2019 – 2022

SKILLS

- Cloud Platforms: GCP, Microsoft 365, Azure AD
- Security & Compliance: PCI DSS, ISO 27001, MFA, DLP, IAM
- Network Infrastructure: SonicWall, VLANs, LAN/WAN, Firewall Management, Network troubleshooting, Switching and Routing
- System Monitoring & Incident Response: Security alerts handling, SIEM tools, IT governance
- SSL Management: Selection, installation, renewal, and optimization of SSL certificates
- Backup & Recovery: Acronis, Altaro, Azure Storage, N-Central

CERTIFICATIONS

- Great Learning : Microsoft Azure Essentials, Cloud Foundation, Introduction to Information Security.
- CISCO : Cybersecurity, Network troubleshooting, Network Addressing & Troubleshooting
- Network Security : NSE 1 & NSE 2
- Backup : Acronis Cloud Associate and Acronis Cloud Tech
- Helpdesk Training : Apex Learning Service Helpdesk and Technical Support

TOOLS & TECHNOLOGY

- Ticketing Tool : Autotask, Freshworks, Connectwise, Zoho, MS365 Dynamics
- Remote Tool : Datto, Goto Assist, Meraki, Connectwise, Splashtop, N-Central
- Password Manager : IT Glue, Keeper
- Backup Management : Altaro, Acronis, Azure Storage, N-Central
- SIEM & Monitoring: Datto, Splunk, Meraki, N-Central

PROFESSIONAL EXPERIENCE

System IT Engineer
RVS iGlobal | 2023 - Present

- Conducted incident response handling using SIEM tools, troubleshooting alerts, and analyzing network logs.
- Implement and support security best practices such as MFA, Conditional Access, DLP, and Microsoft Defender for Office 365.
- Deploy and manage Microsoft Intune for device compliance, endpoint security, and application policies.
- Monitored and managed security alerts and incidents across on-premises and cloud environments.
- Managing Backups on N-able, RMM and OneDrive
- Provided Level 1-3 IT support for server, network, and security issues in GCP, SonicWall, Meraki, ,VPN & other network device.
- Administered Azure AD, Active Directory, and Microsoft 365, ensuring security policies (SPF, DKIM, DMARC, MFA, DLP).
- Developed IT policies, risk management strategies, and compliance documentation.
- Network troubleshooting, Switching and Routing, Firewall, VLANs, LAN-WAN
- Managed firewall rules, VLANs, and network configurations to optimize performance and security.

Trainee IT Engineer
RVS iGlobal | 2022 - 2023

- Managed and configured Active Directory, Azure AD, and M365 Admin Portal.
- Managing and configuring the M365 admin portal and Set-up email security by configuring SPF, DKIM & DMARC.
- Remote Troubleshooting.
- Printer management, Scan to email setup.
- Configuring and Managing Domain server, File Printer, DHCP, DNS, GPO.
- Creating, Managing and Configuring user and devices in Active Directory and MS 365 Admin Center
- Assisted in IT documentation, compliance checks, and security assessments.

PROJECTS

Mastercard Cybersecurity Job Simulation

- Designed and executed phishing email simulations to test cybersecurity awareness.
- Analyzed phishing performance metrics and conducted security training sessions.

ANZ Australia Cyber Security Management

- Investigated suspicious emails and performed risk assessments.
- Analyzed network packet captures to identify potential security threats.