ANKIT MUDGIL

Cybersecurity Professional | IT Support & Systems Administration | MSc Cybersecurity
Dublin, Ireland
+353 899 442 399 | mudgilankit001@gmail.com
Ankit Mudgil | LinkedIn | GitHub (Ankit Mudgil)

PROFESSIONAL SUMMARY

Cybersecurity professional and IT systems specialist with over 3 years of progressive experience spanning IT support, systems administration, and security operations. Holds an MSc in Cybersecurity (2.1 Honours) from National College of Ireland and a Bachelor's in Hardware & Networking (First Class Honours) from Panjab University. Combines deep technical expertise with proven ability to deliver exceptional user support, achieving consistent 98% customer satisfaction ratings while managing complex IT environments.

Experienced across the full spectrum of enterprise IT — from deskside support and helpdesk operations through to server administration, cloud infrastructure, identity management, and security monitoring. Strong hands-on expertise with Microsoft technologies including Windows Server, Active Directory, Azure AD/Entra ID, Microsoft 365, Microsoft Intune, and Autopilot. Skilled in SIEM deployment and tuning, vulnerability assessment, incident response, and security documentation. Demonstrated ability to reduce alert noise by 71% through custom correlation rule development while maintaining detection accuracy.

Proven track record of taking ownership of complex technical issues, working independently with minimal supervision, and collaborating effectively with cross-functional teams. Strong communicator with ability to translate technical concepts for non-technical audiences. Committed to continuous learning and professional development, with Microsoft and CompTIA certifications in progress. Based in Dublin with full Irish work authorisation (no sponsorship required). Available from end of April 2026.

CORE COMPETENCIES

Security Operations: SIEM deployment and tuning (Wazuh, Microsoft Sentinel) | Security alert triage and analysis | Threat detection and escalation | Vulnerability assessment and management | Incident response | Security documentation | Compliance awareness (GDPR, NIS2) | Risk assessment | False positive reduction | Custom correlation rule development | Malware analysis fundamentals

Cloud & Identity Management: Microsoft Azure | Azure AD / Entra ID | Conditional Access policies | Multi-Factor Authentication (MFA) | Single Sign-On (SSO) | SCIM provisioning | Identity lifecycle management | Hybrid identity environments | Azure-hosted servers | Cloud security | AWS fundamentals | IAM configuration

Microsoft 365 Administration: Exchange Online | Microsoft Teams | SharePoint | OneDrive | Outlook | Microsoft Defender | Data Loss Prevention awareness | Licence management | User provisioning | Application troubleshooting | M365 Security Centre | Email flow troubleshooting | Collaboration tools administration

Endpoint Management & MDM: Microsoft Intune | Windows Autopilot | Device enrolment | Compliance policies | Application deployment | Security baselines | Mobile device management | iOS and Android support | BYOD support | Endpoint security | Device lifecycle management | Gold image deployment | System imaging

Windows Server & Infrastructure: Windows Server 2016/2019/2022 | Active Directory administration | Group Policy Objects (GPOs) | Organisational Units (OUs) | DNS server | DHCP server | File server | Print server | User and group management | Permissions management | Server maintenance | Backup management (Veeam) | VMware virtualisation

Networking: TCP/IP configuration | LAN/WAN | DNS configuration | DHCP management | VPN setup and troubleshooting | Wi-Fi configuration and troubleshooting | Network diagnostics | Firewall basics (SonicWall) | Router and switch configuration | Network patching | Wireless installations | Remote access support | Connectivity troubleshooting

Desktop & Hardware Support: Windows 10/11 troubleshooting and support | macOS support | Linux fundamentals | PC and laptop hardware diagnostics | Hardware troubleshooting and repair | Printer setup and maintenance | Peripheral configuration | Mobile device support | Meeting room AV equipment | Video conferencing support | Asset management | Equipment provisioning | Hardware lifecycle management

IT Service Management: ServiceNow | Jira Service Desk | Freshservice | Incident management | Service request handling | Problem management | SLA management and adherence | KPI tracking | Ticket documentation | Escalation handling | First-call resolution | ITIL best practices | Knowledge base creation | Process improvement

Scripting & Automation: PowerShell scripting | Python programming | Bash scripting | Task automation | Diagnostic scripts | Process automation | SQL fundamentals | Machine learning basics (scikit-learn)

Documentation & Communication: Technical documentation | Standard Operating Procedures (SOPs) | User guides | Knowledge articles | Infrastructure diagrams | Asset registers | Security procedural documents | Incident documentation | Training delivery | Non-technical user communication | Vendor coordination | Cross-functional collaboration

PROFESSIONAL EXPERIENCE

System Support Administrator / IT Security Specialist

Fraser Valley India | *University of the Fraser Valley* | *January 2025 – February 2026*

Systems Administration & Infrastructure:

Administered Windows Server 2016/2019/2022 environments including Active Directory, Group Policy, DNS, DHCP, and file/print services for 200+ users across multiple departments

Managed Microsoft 365 tenant including Exchange Online, Teams, SharePoint, and OneDrive — user provisioning, licence management, and application administration

Administered Azure AD/Entra ID including Conditional Access policies, Multi-Factor Authentication, SSO configuration, and hybrid identity management

Deployed and managed Microsoft Intune MDM solution — device enrolment, compliance policies, application deployment, security baselines, and Autopilot provisioning

Maintained both cloud and on-premise infrastructure ensuring systems remained secure, stable, and efficient across hybrid environments

Configured and maintained network infrastructure including routers, switches, Wi-Fi access points, VPN, and firewall configuration

Managed backup solutions using Veeam Backup — ensuring data protection, monitoring backup jobs, and testing restoration procedures

Administered VMware virtualisation environment — virtual machine provisioning, maintenance, and performance monitoring

Security Operations:

Deployed and configured SIEM platform (Wazuh) across 50+ endpoints — achieving 71% reduction in false positives through custom correlation rule development and tuning

Analysed and triaged security alerts from SIEM platform — identifying potential risks, investigating incidents, and escalating as necessary

Conducted vulnerability research on site equipment, network infrastructure, and endpoint devices — assessing security threats and recommending mitigations

Consolidated security reports from multiple risk surfaces including firewalls, endpoint protection, Microsoft 365 security features, and vulnerability assessment tools

Evaluated proposed software solutions for security risks and compliance with organisational policies before deployment

Engaged with vendors to communicate security policies and ensure compliance with data protection and cybersecurity standards

Developed departmental procedural documents based on security policies and scheduled regular reviews to ensure ongoing compliance

Maintained detailed records of security incidents, response actions, and system vulnerabilities for reporting and continuous improvement

IT Support & Service Delivery:

Provided Level 2 deskside and remote support — acting as key escalation point for complex incidents across hardware, software, and network issues

Managed IT onboarding and offboarding processes — provisioning equipment, configuring system access, and ensuring clean account deactivation for leavers

Maintained IT asset inventory — tracking equipment, processing RMAs, coordinating hardware purchases, and managing vendor relationships

Created and maintained technical documentation including SOPs, user guides, knowledge base articles, and infrastructure diagrams

Participated in IT projects including hardware refresh, software rollouts, and infrastructure upgrades — ensuring successful delivery with minimal disruption

Used PowerShell for diagnostic and task automation — streamlining support processes and reducing resolution times

Coordinated with external suppliers and internal teams to resolve issues and maintain service quality

IT Support Engineer

Fraser Valley India | *University of the Fraser Valley* | *May 2022 – December 2024*

Technical Support & Service Desk:

Delivered 1st and 2nd level IT support for 200+ users — achieving 98% customer satisfaction and 95% first-call resolution rate consistently

Managed 100+ support tickets monthly via ITSM platforms (ServiceNow, Jira, Freshservice) — ensuring accurate documentation, SLA adherence, and timely resolution

Monitored service desk queue and prioritised incoming requests — responding to tickets, contacting users, planning workload, and following up on closed tickets

Determined proper escalation paths for complex issues — coordinating with senior engineers, third-party vendors, and internal resolver groups

Provided phone, email, and in-person support — demonstrating excellent communication skills and ability to explain technical issues to non-technical users

Desktop & Hardware Support:

Troubleshot and resolved Windows 10/11 issues including OS configuration, driver problems, application errors, profile issues, and performance diagnostics

Diagnosed and repaired hardware issues on desktops, laptops, printers, and peripherals — performing diagnostics, component replacement, and preventive maintenance

Performed system imaging, software installation, OS updates, and Gold image deployment — supporting new equipment provisioning and system refreshes

Supported mobile devices (iOS, Android) — configuration, troubleshooting, enterprise application support, and MDM enrolment

Supported meeting room AV equipment and video conferencing systems — ensuring reliable operation for business communications

Performed end-user data backup and restoration as required during service incidents and device migrations

Systems & Network Administration:

Administered Active Directory — user account creation, password resets, security group management, OU administration, and permissions configuration

Managed Microsoft 365 applications — Exchange Online, Teams, SharePoint, OneDrive — including user provisioning, troubleshooting, and licence management

Troubleshot network connectivity issues using TCP/IP knowledge — resolving DNS, DHCP, VPN, Wi-Fi, and remote access problems

Supported Windows Server environments — user management, file permissions, Group Policy, print services, and routine maintenance

Monitored client backups and system health — ensuring data protection and proactive issue identification through regular health checks

Documentation & Process Improvement:

Created comprehensive technical documentation including SOPs, user guides, troubleshooting articles, and knowledge base content — reducing repeat tickets by 30%

Maintained accurate IT asset inventory — tracking equipment assignments, managing asset lifecycle, and coordinating hardware refreshes

Supported IT onboarding and offboarding — ensuring new employees had equipment and access on day one, and leavers were cleanly offboarded

Identified repeat issues and contributed to service improvement initiatives — recommending process enhancements and automation opportunities

Demonstrated ability to work independently with minimal supervision while contributing positively to team environment

Retail Assistant (Hospital Shop)

The Coombe Women & Infants University Hospital | August 2025 – Present

Provide excellent customer service in a busy healthcare environment — demonstrating strong interpersonal and communication skills

Work cooperatively with colleagues as part of a team — demonstrating flexibility, reliability, and commitment to service excellence

Gained firsthand understanding of healthcare environment operations and the critical importance of IT reliability in clinical settings

Demonstrate commitment to hospital values including empathy, teamwork, dignity and respect, and always striving to be at our best

EDUCATION

Master of Science in Cybersecurity | 2.1 Honours (Upper Second Class)

National College of Ireland, Dublin | September 2023 – May 2025

Core Modules: Security Risk Management, Network Security, Digital Forensics, Incident Response, Security Governance, Vulnerability Assessment, Compliance Frameworks, Threat Intelligence, Cloud Security, Cryptography

Research Focus: SIEM tuning and optimisation, Machine learning for phishing detection, Malware analysis techniques

Bachelor of Vocation in Hardware & Networking | 1st Class Honours

GGDSD College, Panjab University, India | July 2019 – July 2022

Core Modules: Computer Hardware, Networking Fundamentals, Operating Systems, System Administration, Technical Support, PC Maintenance, Network Configuration, Server Administration

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

In Progress:

MD-102: Microsoft Endpoint Administrator — Managing modern Windows 10/11 deployment, device management, and endpoint security

SC-900: Microsoft Security, Compliance, and Identity Fundamentals — Core concepts of security, compliance, and identity across Microsoft cloud services

CompTIA Security+ — Baseline cybersecurity skills for security and network administrators

TECHNICAL PROJECTS

SIEM Tuning & Threat Detection — Wazuh Implementation

GitHub: github.com/Mudgil-A/SIEM-Tuning-Wazuh-SME

Deployed and configured Wazuh SIEM platform across 50+ endpoints in an SME environment. Developed custom correlation rules to reduce alert noise by 71% while maintaining detection accuracy. Implemented real-time monitoring dashboards and automated alerting for critical security events. Created comprehensive documentation for ongoing management and rule refinement.

Technologies: Wazuh, ELK Stack, Linux, PowerShell, Security Operations

Phishing Detection via Machine Learning

GitHub: github.com/Mudgil-A/Phishing-Detection-ML

Developed a phishing URL detection system using machine learning classifiers (Random Forest, SVM) as part of MSc Cybersecurity research. Achieved 97% detection accuracy through feature engineering and model optimisation. Processed and analysed large datasets of legitimate and malicious URLs. Created visualisations and documentation of methodology and results.

Technologies: Python, scikit-learn, pandas, Machine Learning, Threat Intelligence

AWS WordPress Security Hardening

GitHub: github.com/Mudgil-A/AWS-WordPress-Security

Secured a cloud-hosted WordPress deployment on AWS by identifying and mitigating vulnerabilities. Implemented IAM best practices, network security controls, and application-layer protections. Configured security groups, NACLs, and WAF rules. Documented security posture improvements and ongoing monitoring recommendations.

Technologies: AWS (EC2, IAM, VPC, WAF), WordPress, Cloud Security, Network Security

Malware Analysis — WannaCry Ransomware

GitHub: github.com/Mudgil-A/Malware-Analysis-WannaCry

Conducted static and dynamic analysis of the WannaCry ransomware in a controlled lab environment. Documented attack mechanisms, propagation techniques, and indicators of compromise. Analysed encryption routines and network communication patterns. Created detailed technical report with defensive recommendations.

Technologies: Malware Analysis, Reverse Engineering, Sandbox Environment, Threat Research

KEY ACHIEVEMENTS

Achieved 98% customer satisfaction rating consistently while managing 100+ support tickets monthly — demonstrating exceptional service delivery and communication skills

Reduced SIEM alert noise by 71% through custom correlation rule development — enabling security team to focus on genuine threats while maintaining detection accuracy

Maintained 95% first-call resolution rate — exceeding service desk KPIs and minimising user downtime through effective troubleshooting

Developed machine learning phishing detection system achieving 97% accuracy — contributing to academic research in cybersecurity threat detection

Created comprehensive technical documentation reducing repeat tickets by 30% — improving team efficiency and enabling self-service resolution

Deployed Microsoft Intune MDM solution with Autopilot — streamlining device provisioning, improving security compliance, and reducing deployment time

Successfully managed complex device migrations with zero data loss — ensuring minimal disruption and positive user experience during technology transitions

Contributed to hardware refresh projects and software rollouts — ensuring successful delivery through planning, testing, and stakeholder communication

TECHNICAL TOOLS & PLATFORMS

Security: Wazuh | Microsoft Sentinel | Microsoft Defender | Nessus | Burp Suite | Wireshark | OWASP ZAP | Nmap | Metasploit (fundamentals)

Microsoft: Windows Server 2016/2019/2022 | Active Directory | Azure AD / Entra ID | Microsoft 365 | Exchange Online | SharePoint | Teams | Intune | Autopilot | SCCM (familiar) | Group Policy

Cloud: Microsoft Azure | AWS (fundamentals) | Azure AD | Conditional Access | MFA | SSO | SCIM

Virtualisation & Backup: VMware vSphere | Hyper-V (fundamentals) | Veeam Backup & Replication | VirtualBox

Networking: TCP/IP | DNS | DHCP | VPN | SonicWall (fundamentals) | Cisco (fundamentals) | Wi-Fi configuration | Network diagnostics

ITSM & Ticketing: ServiceNow | Jira Service Desk | Freshservice | Freshdesk | Confluence

Remote Support: TeamViewer | AnyDesk | Microsoft Remote Desktop | Quick Assist

Scripting & Development: PowerShell | Python | Bash | SQL | Git | VS Code

Operating Systems: Windows 10/11 | Windows Server | macOS | Linux (Ubuntu, CentOS, Kali) | iOS | Android