

ASHISH SHARMA

Infrastructure & Security Engineer

Faridabad, Haryana, India | +91 93158 01820 | ashish.alive2@gmail.com | linkedin.com/in/ashish-in

PROFESSIONAL SUMMARY

Infrastructure security professional with 5+ years securing multi-site enterprise environments: SIEM-based threat detection (Wazuh), firewall and VPN hardening, Active Directory access control, patch management, and RCA-driven incident response. Works hands-on with controls rather than on paper: has mapped technical controls to SOC 2 Trust Services Criteria and ISO 27001:2022, built audit-ready evidence and access-review workflows, and secured AWS workloads with least-privilege IAM, centralised logging, and encryption. Clear written communicator through RCA reports, runbooks, and incident logs. ISC2 Certified in Cybersecurity (CC); preparing for AWS Certified Solutions Architect – Associate.

PROFESSIONAL EXPERIENCE

System & Network Administrator

May 2025 – Present

Ram Rattan Group · Gurgaon, India

- Designed and secured enterprise LAN/WAN/WLAN infrastructure with SSID segmentation for staff/guest separation; configured Sophos firewall policies and site-to-site/remote-access VPNs, and administered Cisco routers/switches.
- Led Root Cause Analysis (RCA) and problem management for critical incidents, reducing mean time to recovery and implementing corrective controls to prevent recurrence.
- Administered Active Directory for a 50-user environment: user onboarding/offboarding, group-based least-privilege access, and password/account policies; managed HPE ProLiant, Linux, and Windows Server 2019 hosts on a regular patch cadence.
- Automated routine administrative tasks via PowerShell/Bash scripts, reducing manual workload and improving system uptime.
- Administered ERP (4QT) and HR (Pinga) platforms, including role-based user access and data-integrity checks across departments.
- Provided technical coaching to junior staff and contributed to internal knowledge-sharing sessions.

System & Network Administrator

Oct 2021 – Apr 2025

MVL Limited · Gurgaon, India

- Deployed and managed multi-site LAN/WAN across Gurgaon & Yamunanagar, serving 200+ users.
- Implemented Farvision ERP and Zing HR systems end-to-end, streamlining procurement, finance, and HR workflows across departments.
- Hardened the IT environment with Sophos firewalls, VPNs, and endpoint protection; ran periodic compliance audits and tracked findings through to remediation, reducing security incidents through layered defence controls.
- Deployed and maintained Zabbix & PRTG monitoring for servers, network devices, and applications — enabling proactive incident response and reducing unplanned downtime.
- Conducted incident response, RCA documentation, and root-cause remediation for Severity 1/2 outages; maintained a structured incident log improving resolution time over tenure.
- Partnered with leadership on IT strategy and budgeting; evaluated vendor proposals against security and compliance requirements and renegotiated contracts, cutting procurement costs by ~25%.

Desktop Engineer

Apr 2020 – Sep 2021

CPS Interior Pvt. Ltd. · Faridabad, India

- Delivered L1/L2 support for hardware, OS, and business applications, reducing end-user downtime through structured ticketing and SLA adherence.
- Implemented scheduled backup routines using Cobian Backup for critical business data, ensuring recovery point objectives were met.

KEY PROJECTS

SOC 2 Readiness & Control Mapping

Personal Project · 2026

Built a SOC 2 readiness toolkit mapping Wazuh, Active Directory, Sophos, and AWS controls to the Trust Services Criteria (CC6 access, CC7 monitoring, CC8 change management) with ISO 27001:2022 Annex A cross-references; produced a control matrix, evidence checklist, access-review template, risk register, and IR runbook.

SOC 2 TSC · ISO 27001:2022 · Control Matrix · Risk Register · GitHub

AWS Security Baseline Lab <i>Personal Project · 2026</i>	Hardened an AWS account to a SOC 2-aligned baseline: least-privilege IAM roles with enforced MFA, multi-region CloudTrail, AWS Config rules, GuardDuty threat detection, S3 Block Public Access with SSE-KMS encryption, and Secrets Manager. Scanned lab hosts with OpenVAS and ran a GoPhish phishing simulation, triaging findings and tracking remediation to closure. <i>AWS IAM · CloudTrail · Config · GuardDuty · KMS · Secrets Manager · OpenVAS · GoPhish</i>
SIEM Implementation <i>Freelance · 2024</i>	Deployed Wazuh SIEM from scratch: installed manager/agents, wrote custom detection rules, configured FIM, and built PCI-DSS/NIST compliance dashboards. <i>Wazuh · Elastic Stack · Log Analysis</i>
Zabbix Monitoring Deployment <i>2022</i>	Built end-to-end monitoring solution with auto-discovery, custom triggers, and automated alerting for servers, switches, and applications. <i>Zabbix · SNMP · Automation · Dashboards</i>
Azure Blob Storage <i>Cloud Infrastructure · 2023</i>	Configured RBAC policies, access tiers (Hot/Cool/Archive), lifecycle management rules, and compliance controls for scalable, cost-optimised cloud storage. <i>Azure · IAM/RBAC · Lifecycle Policies</i>
Enterprise Network Deployment <i>MVL Limited · 2021–2025</i>	Architected a two-site LAN/WAN rollout; coordinated third-party vendors, led compliance checks, and trained staff. <i>Cisco · Sophos · Windows/Linux · Hyper-V/VMware</i>
OpenEstate — Real Estate CRM <i>Open-Source Project · 2026</i>	Built a self-hostable, multi-tenant real-estate CRM (~70K-LOC TypeScript monorepo) with database-level tenant isolation via PostgreSQL row-level security and an append-only financial ledger. <i>TypeScript · NestJS · React · PostgreSQL/RLS · Redis · CI/CD</i>

TECHNICAL SKILLS

Networking	TCP/IP · DHCP · DNS · VLANs · LAN/WAN · VPN (IPsec/SSL) · Routing & Switching · Cisco IOS · Sophos Firewall
Systems	Windows Server 2019 · Active Directory · Linux (CentOS/Ubuntu) · VMware ESXi · Hyper-V · HPE ProLiant · PowerShell/Bash Scripting
Security	Wazuh SIEM · IDS/IPS · Endpoint Protection · Vulnerability Scanning (OpenVAS) · Phishing Simulation (GoPhish) · Security Audits · Risk Assessment
Compliance & GRC	SOC 2 (Trust Services Criteria) · ISO 27001:2022 Annex A · NIST · PCI-DSS · Control Mapping · Evidence Collection · Access Reviews · Risk Register · Vendor Risk
Cloud & Backup	AWS (IAM, CloudTrail, Config, GuardDuty, KMS, Secrets Manager, EC2, S3, VPC) · Azure Blob Storage & RBAC · Veeam Backup · Synology NAS
Monitoring	Zabbix · PRTG · Wireshark · GLPI · IP-CCTV
ERP / Business	Farvision ERP · Zing HR · 4QT · Pinga · Microsoft 365 · SharePoint · NEC SL2100 IP-PBX
Operations	Incident Management · RCA / 5 Whys · Change Management · Vendor Management · IT Budgeting · Staff Training

EDUCATION & CERTIFICATIONS

Bachelor of Science in Data Science
IIT Madras (Online) — Pursuing | Expected 2028

Diploma, Electrical Engineering
Govt. Polytechnic, Lisana Rewari | 2018 – 2021

Certifications

- ISC2 Certified in Cybersecurity (CC) — Jun 2026
- AWS Certified Solutions Architect – Associate — In Progress
- Fortinet Certified Fundamentals Cybersecurity — Jan 2026
- Fortinet NSE 1 — Network Security Associate & Threat Landscape
- Exchange Server 2019 — Udemy, Jan 2022
- Linux Foundation Certified System Administrator (LFCS) — In Progress