Mustafa K. Durrani

4 Wainwright Drive, Ajax | 647 394 5690 | linkedin.com/in/mustafakdurrani | mail@mostafadurrani.com | mostafadurrani.com

SOC Analyst with CompTIA Security+ and ISC² Certified in Cybersecurity, and hands-on experience building a home SIEM lab using Wazuh. Background in endpoint security and incident triage, with over 1 year of professional experience in incident response and compliance auditing across a 150-server environment.

Professional Experience

Resident Engineer (SOC Level 1 Analyst) **Feb. 2026 — Present**
Secure Networks — *Lahore, Pakistan*

- Managed endpoint security operations for ~150 servers across PITC's multi-segment infrastructure, maintaining agent health, policy compliance, and system availability across mixed Linux and Windows Server environments.
- Monitored and triaged ~200 security events weekly across Integrity Monitoring, Log Inspection, Firewall, and IPS modules, and investigated alerts including active reconnaissance probes, brute-force authentication attempts, and vulnerability exploitation attempts.
- Coordinated with SOC and IT teams to drive incident response and containment, performing root cause analysis on security incidents and system issues to prevent recurrence.
- Diagnosed and resolved Deep Security agent connectivity failures, policy conflicts, and multi-error states across distributed network segments, restoring managed status to degraded endpoints.
- Delivered structured operational reporting (weekly and monthly) and maintained documentation of incidents, system changes, and troubleshooting procedures.

Junior Cybersecurity Consultant **Mar. 2025 — Feb. 2026**
Softbiz Solutions *— Plano, Texas (Remote from Lahore, Pakistan)*

- Conducted comprehensive audits of information systems using Center for Internet Security (CIS) benchmarks to evaluate compliance and identify ~22 security gaps ranging from trivial to critical.
- Deployed and configured 12 PowerEdge servers and SAN switches, from physical rack installation, cabling, and asset inventory to Proxmox cluster deployment, as well as decommissioning of old equipment.
- Implemented and configured multi-factor authentication (MFA) protocols on high-risk endpoints (PC and mobile) via Google Authenticator.
- Identified and documented a recurring malware infection pattern, collaborating with security team to develop and implement USB device controls.

Education & Certifications

York University, ON, Canada - *BSc. Computer Science* **Oct. 2024**
ISC2 Certified in Cybersecurity *(CC)* **Feb. 2025**
CompTIA Security+ *(SY0-701)* **May 2026**

Projects

Home Lab: SIEM Threat Detection & Response Environment

- Built a full-cycle detection lab using Wazuh SIEM, Windows/CentOS agents, a honeypot, and a Kali Linux attacker.
- Simulated attacks, wrote detection rules, and documented full build with screenshots and analysis.

Skills

- Wazuh (SIEM), Trend Micro Deep Security / Apex One
- Threat Detection & Hunting
- Incident Response
- MITRE ATT&CK Framework
- Cross-Team Collaboration
- Python / PowerShell / SQL
- IPS / IDS Monitoring
- Log Analysis and Inspection
- Vulnerability Assessment
- SAN Configuration
- Linux / CentOS / Ubuntu
- Network Security Monitoring
- Firewall Rule Analysis
- Network Log Analysis
- NIST CSF / CIS Controls
- Inventory / Asset Management
- System Administration