Awaise Choudhary

Cybersecurity Analyst | Vulnerability Management | SecOps
Email: awaisetech00@gmail.com | **GitHub**: https://github.com/awaisetechgit
LinkedIn: https://www.linkedin.com/in/awais-c/ | **Portfolio**: https://awaisetech.com/

PROFESSIONAL SUMMARY:

Cybersecurity analyst with hands-on experience in vulnerability management and SOC operations across enterprise environments.Core expertise in executing and managing Tenable vulnerability scans, validating findings, prioritizing risk using CVSS and asset context, and coordinating remediation with IT teams to meet SLA and compliance requirements.Background in SOC alert triage and junior-level threat hunting using Microsoft Sentinel and Defender, providing strong context on how vulnerabilities translate into real-world security incidents

EXPERIENCE:

Company: Layer Seven Security Sept/2025 - Dec/2025
Title: SOC Analyst I (Vulnerability Management)

- Executed continuous **agent-based Tenable vulnerability scans** across **300+ Windows and Linux assets**, supporting post-patch validation and closure of critical and high-risk findings within SLA.
- Validated vulnerability findings by verifying patch levels, software versions, and configuration states, reducing false positives and improving remediation accuracy.
- Prioritized vulnerabilities using **CVSS severity, asset criticality, and exposure context**, ensuring remediation efforts targeted highest-risk systems.
- Collaborated with IT and infrastructure teams to track remediation progress, verify patches, configuration changes, and software updates through system validation and rescans to ensure vulnerabilities were properly resolved before closure.
- Documented vulnerability findings and remediation status in **Jira**, supporting **SOC 2 and PCI DSS** audit requirements.
- Assisted with asset discovery and continuous vulnerability monitoring to improve visibility of newly introduced systems.
- Supported SOC operations by triaging security alerts and participating in threat hunting activities as needed.

Company: Layer Seven Security Apr/2025 - Aug/2025
Title: Cybersecurity Intern – SecOps

- Conducted proactive threat hunting activities across **300 endpoints**, identifying indicators of compromise and escalating validated findings.
- Developed and tested **custom SIEM detection rules and dashboards** in collaboration with senior analysts, improving SOC visibility into suspicious activity.
- Investigated security alerts, documented findings, and escalated confirmed incidents with clear evidence and context, improving triage efficiency.
- Supported firewall rule reviews and security configuration updates to reduce attack surface.
- Participated in tabletop exercises and simulated incident response scenarios to reinforce SOC workflows and escalation procedures.

Company: Proline Consulting Jun/2024 - Feb/2025
Title: Server Administrator – Security & Systems

- Provided technical support for hardware, software, and network issues, resolving user tickets within defined SLA targets while maintaining accurate documentation.
- Administered user accounts, group memberships, and access permissions in Active Directory, enforcing least-privilege access and supporting onboarding/offboarding processes.
- Supported operating system and application patch deployments, verifying successful updates and helping reduce operational downtime and security exposure.
- Tracked incidents, service requests, and change activities using ServiceNow and Jira, ensuring proper categorization, escalation, and audit-ready records.
- Performed basic network troubleshooting, including DNS resolution issues, DHCP address assignment, and connectivity problems, escalating complex issues to senior engineers when required.

TECHNICAL PROJECTS

GitHub Portfolio: https://github.com/awaisetechgit (Documentation of labs, scripts, and security projects)

Vulnerability Management & Threat Hunting Lab

Tools: Tenable.io, Microsoft Sentinel, Defender for Endpoint, Azure VMs, KQL

- Executed vulnerability scans, validated findings, and practiced remediation verification workflows.
- Built SIEM dashboards and KQL queries to support threat detection and investigation.
- Implemented firewall rules and network segmentation to reduce lateral movement risk.

Home SOC Lab

Tools: Proxmox, pfSense,

- Built a virtualized SOC environment with segmented networks to simulate enterprise security architecture.
- Practiced identity and access management using Active Directory.
- Tested detection and response workflows across SIEM and EDR tooling.

CERTIFICATIONS & EDUCATION

B.S. Cybersecurity & Information Assurance — Western Governors University *(In progress)*

Certifications:

- CompTIA Security+
- Microsoft Azure Fundamentals (AZ-900)
- Microsoft Azure Security Engineer Associate (AZ-500)
- AWS Cloud Practitioner
- ISC² Certified in Cybersecurity (CC) *(In Progress)*

ADDITIONAL SKILLS AND TECHNOLOGIES

Incident response, threat detection, alert triage, network monitoring, system log analysis, vulnerability assessment, firewall/IDS/IPS management, endpoint detection and response (EDR), PAM solutions, patch management, CVE/CWE management, NIST Cybersecurity Framework, SOC 2/GDPR compliance, analytical problem-solving