ASHISH GHIMIRE

+1 (318) 507-4123 ◇ Shreveport, Louisiana
ashishghmr1998@gmail.com ◇ linkedin.com/in/ashish-ghimire-96755b179

SUMMARY

Driven Cybersecurity Engineer with over 3 years of experience fortifying enterprise defenses through advanced threat detection, incident response, and adversary emulation. Skilled in SIEM (Splunk, QRadar), EDR (CrowdStrike Falcon), and network security tools (Palo Alto, Cisco ASA, Fortinet). Experienced in penetration testing, red teaming, vulnerability management, and cloud security. Adept in scripting with Python, Bash, and PowerShell to automate defensive controls. Deep understanding of MITRE ATT&CK, compliance standards, and proactive threat intelligence.

SKILLS

- **Security Operations:** Threat Detection, SOC Operations, Splunk, Splunk SOAR, Splunk Dashboards, CrowdStrike Falcon, Microsoft Entra ID
- **Incident Response:** Triage & Containment, Malware Analysis, Log Forensics, Playbook Development
- **Penetration Testing:** Nmap, Burp Suite, Metasploit, Cobalt Strike, BloodHound, Mimikatz
- **Vulnerability Management:** Nessus, Qualys, OpenVAS, Patch Management, Risk Remediation
- **Network Security:** Palo Alto, Fortinet, Cisco ASA, VPN (IPSec, Site-to-Site, DMVPN), IDS/IPS, Wireshark, Suricata, Zeek, Snort
- **Cloud Security:** AWS, Azure Security, IAM, OAuth, Kerberos, Zero Trust
- **Threat Hunting:** Splunk Dashboards, YARA, Threat Intel Feeds, NetFlow, PCAP Analysis
- **SIEM & Logging:** Splunk (correlation rules, dashboards), QRadar, ELK Stack
- **Systems Administration:** Linux/Windows Hardening, Active Directory, Group Policy, Backup/Recovery
- **Identity & Access Management:** MFA, SSO, SAML, PAM, Entra ID Integration
- **DevOps & Infrastructure:** Docker, Kubernetes, Terraform, Ansible, GitHub Actions CI/CD
- **Virtualization:** VMware ESXi, Proxmox, Hyper-V, Cloud Networking
- **Compliance & Governance:** ISO 27001, SOC 2, HIPAA, GDPR, PCI DSS, NIST CSF
- **Programming:** Python, Bash, PowerShell

EXPERIENCE

Student SOC Analyst Oct 2024 – Present
Louisiana State University Shreveport

- Handled and triaged 100+ escalated security alerts per month in Splunk SOAR, including phishing attempts, brute-force attacks, and firewall blocks, while maintaining 100% SLA adherence for critical incidents.
- Investigated escalated cases by correlating logs across CrowdStrike Falcon, Microsoft Azure, and Palo Alto firewalls, providing actionable threat intelligence and reducing mean time to resolution (MTTR) by 30%.
- Built and optimized 15+ custom Splunk dashboards and reports using MITRE ATT&CK Heatmap, Machine Learning Toolkit, and Security Essentials to enhance threat detection and compliance tracking.
- Conducted in-depth analysis of 50+ security incidents, leveraging Tenable vulnerability insights and Falcon EDR to remediate attack vectors, strengthen endpoint defenses, and prevent recurrence.

Security Research Analyst Aug 2023 –Dec 2023
Security Pal, Inc.

- Conducted 20+ comprehensive risk assessments and compliance audits for Fortune 500 clients, including OpenAI, monday.com, and Figma, ensuring 100% adherence to GDPR, HIPAA, ISO 27001, NIST, and SOC 2 standards.
- Collaborated with cross-functional engineering, product, and compliance teams to align security initiatives with business goals, accelerating audit readiness and reducing remediation timelines by 25%.
- Produced executive-ready reports with actionable risk mitigation strategies that strengthened overall client security posture and supported successful certification renewals.

Network Security Engineer Jan 2020 – Jul 2023
Max International Pvt. Ltd.

- Deployed & maintained 30+ Palo Alto NGFWs, FortiGate firewalls & Cisco ASA devices, achieving 99.9% uptime and blocking hundreds of threats monthly.
- Configured and managed enterprise-grade routers & switches (Layer 2/3), implementing VLANs, routing protocols, ACLs, and NAT to ensure secure, reliable connectivity.
- Designed and implemented VPN solutions including IPSec remote-access, Site-to-Site VPNs & Cisco DMVPN, supporting 500+ remote and branch users with ISO 27001 compliance.
- Created & enforced granular firewall & security policies using SSL/TLS decryption, intrusion prevention (IPS/IDS), URL filtering, content filtering, WildFire malware analysis & reputation-based blocking to defend against advanced threats.
- Executed 50+ penetration tests & vulnerability assessments (Nessus, Burp Suite, Nmap), reducing critical risks by 40%.
- Monitored, troubleshot & optimized WAN/LAN, firewall & VPN performance, reducing downtime and improving reliability.
- Administered Windows & Linux servers, performing patch management, OS upgrades, user/group administration, Active Directory/GPO management & system hardening.
- Collaborated with IT & compliance teams on server baselines, backup/recovery procedures & access control reviews, helping pass ISO 27001 & PCI DSS audits with zero major findings.

IT Analyst Intern Jul 2018 – Dec 2018
Loop Networks Pvt. Ltd.

- Handled 10–15 customer support calls per day, troubleshooting ISP connectivity issues such as router misconfigurations, dropped connections, and firewall blocks.
- Assisted in configuring and maintaining 20+ routers, switches, and firewalls under supervision, supporting small business and residential customers.
- Logged and tracked 100+ support tickets, ensuring accurate documentation of recurring issues and their resolutions.
- Collaborated with a 4-member IT team, escalating complex cases to senior engineers and contributing to faster resolution of network outages.

hyperref

CERTIFICATIONS

AWS Solutions Architect Associate (SAA)
CompTIA CySA+
CompTIA Security+
CompTIA Network+
ISC2 Certified in Cybersecurity (CC)

PROJECTS

- **Phishing Detection with Machine Learning.** Built a phishing URL classifier using feature engineering (URL length, entropy, domain reputation) and ML models (Random Forest, Logistic Regression), achieving 95% detection accuracy on test data.
- **Network Intrusion Detection System.** Developed a deep learning–based IDS (CNN + LSTM) to classify anomalous traffic patterns; improved zero-day attack detection rates compared to traditional signature-based systems.
- **Active Directory Attack Simulation Lab.** Designed a red-team home lab using Kali Linux + Windows Server AD to simulate Kerberoasting, lateral movement, and credential harvesting attacks; integrated Wazuh + ELK Stack for centralized logging, monitoring, and alerting.

LEADERSHIP

Co-Founder, Kumari.AI 2025 – Present

- Co-founded an intelligent AI routing platform that dynamically selects and unifies multiple LLMs for optimal performance.
- Led a multidisciplinary team (engineering, design, marketing), overseeing hiring, operations, and execution.
- Shaped product vision, GTM strategy, and brand identity, driving early user adoption and market traction.
- Collaborated with investors and stakeholders to refine roadmap and prioritize high-impact features.

EDUCATION

Louisiana State University Shreveport Expected May 2026
MS in Computer Science, Concentration in Cybersecurity
London Metropolitan University March 2021
BSc (Hons) Computer Networking and IT Security