Yaman Shrestha

Austin, Texas • +1-(816)-200-4388 • yamanshrestha08@gmail.com • linkedin.com/in/yaman-shrestha • github.com/yamanshrestha

Summary

Security Analyst with 3+ years of experience in SOC operations, incident response, and threat triage. Experienced in analyzing logs and network traffic (Splunk, Wireshark, Zeek) to identify malicious activity across enterprise environments. Proven ability to investigate alerts following NIST SP 800-61 standards and reduce false positives through data-driven analysis. Hands on experience in phishing and malware analysis.

Professional Experience

Security Focused - Research Assistant, *University of Central Missouri* *Warrensburg, MO | Aug 2024 – Dec 2025*

- Analyzed network traffic using Tshark, Tcpdump, and Wireshark, classifying brute force, SQL injection, DDoS attacks within network telemetry data.
- Performed feature reduction of TCP/IP headers improving signal quality by 75%, achieving 98% accuracy for incident classification.
- Investigated network security incidents, conducting root cause analysis to identify attack vectors using CICIDS2017 and UNSW-NB15 datasets, analyzing 200,000+ rows of packet data.
- Evaluated LLM-based detection, comparing Llama3 and Mistral event classification against classical methods, achieving 17% accuracy improvement for incident classification.
- Streamlined Python automation to parse PCAP files, extract indicators, standardize analysis workflows, and automate LLM fine-tuning, reducing training time by 24 hours per session.

Security Analyst, Syvar *Technology Pvt. Ltd.* *Lalitpur, Nepal* | Apr *2022 – Dec 2023*

- Enhanced SOC operations by performing alert triage, investigation, escalation, and remediation across enterprise environments; detected and responded around 15+ security incidents.
- Conducted vulnerability assessments using Nessus Essentials and Nmap, collaborating with engineering team to remediate 32/35 vulnerabilities, achieving a 91% remediation rate.
- Improved incident response by authoring documentation and designing a playbook for phishing and DDoS attacks, improving team efficiency by 20%.

Security Research Analyst, *SecurityPal Inc.* *Kathmandu, Nepal* **|** *May 2021 – Mar 2022*

- Evaluated security controls across cloud and SaaS environments, reviewing IAM, network security, and data protection controls against ISO 27001 and NIST, PCI-DSS standards.
- Analyzed and answered 300+ of third-party security assessments for enterprise clients, documenting control gaps and risk-based remediation recommendations.
- Collaborated with a team of 10 members to correlate the vendor risk assessment findings and share the with the other pods.

Technical Project

Splunk SOC & Threat Hunting Lab

- Developed and tuned SPL queries aligned with MITRE ATT&CK techniques, detecting lateral movement and privilege escalation while reducing false positives by ~45%.
- Integrated AWS CloudTrail, Sysmon, and Zeek telemetry into Splunk Enterprise, centralizing security event visibility and enabling real-time incident detection across 5 endpoints.
- Developed incident response playbooks that automated low-fidelity alert enrichment using VirusTotal, GeoIP, and AbuseIPDB, reducing initial alert triage time by ~40%.
- Designed interactive **Splunk Dashboards** to visualize network traffic trends and high-priority alerts, reducing the time required to scope and investigate simulated security incidents.

Skills

- **SOC Operations & SIEM**: Splunk (SPL), Wazuh, ELK Stack, Alert Triage & Investigation, Log Correlation, Phishing Analysis, Malware Analysis, IOC Extraction, LLM Incident Classification.
- **Network & Endpoint Security:** Wireshark, Zeek, TCP/IP, DNS, TLS, Windows Event Logs, Active Directory (AD), Firewall/WAF Logs, IDS/IPS Analysis, AWS CloudTrail, Azure Monitor.
- **Incident Response & Frameworks:** NIST SP 800-61, MITRE ATT&CK, NIST CSF, Cyber Kill Chain, OWASP Top 10, STRIDE, Vulnerability Management (CVSS).
- **Automation & Scripting:** Python (Automation/Data Analysis), PowerShell, Bash, Regex, SOAR workflows, n8n, API Integration.

Certifications

CompTIA Security+ • AWS Certified Solutions Architect – Associate • ISC2 Certified in Cybersecurity (CC) • CCNA (Cisco Certified Network Associate) - Course

Education

MS. in Cybersecurity and Information Assurance Lee's Summit, MO
University of Central Missouri Jan. 2024 – Dec 2025

BSc. Computer Networking & IT Security Kathmandu, Nepal
London Metropolitan University *Aug 2018 – Dec 2021*