

Yaman Shrestha

121 E Hunt Ave, 64093, MO

Phone: +1-(816)-200-4388

Email: yamanshrestha08@gmail.com

Social: linkedin.com/in/yaman-shrestha, github.com/yamanshrestha

Summary

Security Analyst and SOC-focused cybersecurity professional with experience in incident detection, vulnerability management, and cloud/network security. Hands-on with SIEM (Splunk, ELK, Wazuh), log analysis, and endpoint/network forensics, plus third-party risk assessments for enterprise clients. Published in IEEE for AI-driven security research. Actively seeking SOC, Security Analyst, or Detection Engineer roles.

Skills and Technical Background

- SOC and Threat Detection:** Real-time alert triage, log correlation (Splunk, ELK, Wazuh), IOC/TTP analysis, threat hunting, threat modelling (STRIDE, PASTA), detection rule writing (Sigma, YARA), MITRE ATT&CK, Cyber Kill Chain, incident documentation & escalation.
 - Incident Response:** Containment, Root Cause & Timeline Analysis, Malware & Phishing Response, Forensic Log Review, Post-Incident Reporting (NIST SP 800-61, PICERL)
 - Network and System Security:** TCP/IP, **Wireshark**, Zeek, Tshark, Nmap, packet analysis, secure network design, VPNs, SSL/TLS, IPv4/IPv6, Windows Event Logs, Traffic Monitoring
 - Vulnerability Management & Cloud Security:** Vulnerability scanning (OpenVAS, NVD CVE API), risk evaluation, AWS, Azure, Google Cloud, DigitalOcean, Akamai (IAM controls, monitoring, hybrid environments).
 - Programming & Automation:** Python, Bash, Regex, Scapy, Security Automation (n8n, Power Automate), Workflow & Alert Enrichment Scripts
 - AI and Security Research:** Machine Learning for Threat & Anomaly Detection (Decision Tree, Random Forest, SVM, KNN), Responsible AI Evaluation, LLM Fine-tuning (Llama, Gemma, Mistral), Explainable AI (SHAP, LIME, XAI), Threat Intelligence NLP, IoT Fingerprinting, AI-Driven Incident Classification & Behavioral Analysis
 - Collaboration and Leadership:** Cross-functional Team Management, Secure SDLC, Policy Documentation, Risk Analysis, Agile/Waterfall Environments, Communication & Escalation Management
-

Certifications

- CompTIA Security+
 - Certified in Cybersecurity (CC) - (ISC)2
 - TryHackMe - SOC Level 1 – (In progress)
 - CCNA (Cisco Certified Network Associate) - Course
 - TCP/IP and Advanced Topics
 - Learning Cloud Computing: Core Concepts
-

Education

University of Central Missouri,

Lee's Summit, MO

MS in Cybersecurity and Information Assurance

Jan. 2024 – Present

Thesis: *Large Language Models for Network Security*

Coursework: Ethical Hacking, Computer Forensics, Threat Intelligence, Cryptography, Advanced Networking, Cyber Policy & Risk Management, Artificial Intelligence

Islington College (London Metropolitan University),

Kathmandu, Nepal

BSc. (Hons) Computer Networking & IT Security

Aug 2018 – Dec 2021

Thesis: *Comparative Analysis of Digital Signatures Using Public Key Cryptography*

Achieved a strong foundation in CCNA Networking, Information Systems, Digital Crime Investigation, and Communication Engineering, focusing on network architecture, secure system design, and cybersecurity principles.

Work Experience

AI/LLM Research Assistant

University of Central Missouri – Warrensburg, MO

Aug 2024 – Present

- Conducting in-depth research on network security, including TCP/IP packet analysis, IoT fingerprinting, **incident detection** techniques aligned with SOC practices.
- Fine-tuning** LLaMA 2 7b, LLaMA 3, Mistral, Gemma models with IoT and incident datasets for security use cases.
- Applying Explainable AI (XAI), LIME and ABC Optimization to streamline security data analysis, reducing feature sets by 75% while maintaining high detection accuracy up to **98%**.
- Evaluating performance comparison with **Deep Learning models** proving **17%** better results with **LLMs**.
- Developing an automated IoT device identification method using **SSL/TLS handshake analysis**, achieving **98.9% accuracy** and outperforming the industry-standard **JA3 hashing method** (18% to 98.9% accuracy)
- Performing LLM evaluation on Llama, Gemma, Mistral.

Security Analyst

Syvar Technology Pvt. Ltd. – Lalitpur, Nepal

Apr 2022 – Dec 2023

- Conducted **vulnerability scanning and risk assessments** to identify and remediate security gaps across client infrastructures.
- Collaborated with developers in an **Agile environment** to implement secure coding practices and perform code reviews aligned with OWASP Top 10.
- Designed and delivered internal **training on incident response, secure SDLC, and security policy compliance**, improving team awareness and security maturity.
- Engaged with **client onboarding and security consultation**, advising on risk mitigation strategies and compliance with NIST CSF and ISO 27001 frameworks.
- Implemented, monitored, and continuously improved **security controls and automation workflows** to strengthen organizational resilience.

Security Research Analyst

SecurityPal Inc. – Baluwatar, Nepal

May 2021 – Mar 2022

- Conducted over 200 third-party risk assessment questionnaires for Fortune 500 companies, ensuring compliance with ISO 27001, NIST CSF, GDPR, HIPAA, PCI-DSS, and CCPA standards.
- Augmented the information to a centralized knowledge base for risk assessment, compliance tracking, and third-party onboarding.

Projects

AI-Powered Endpoint Threat Detection Agent (*In Progress*)

- Building a real-time endpoint anomaly detection agent using Half-Space Trees, surfacing the top 1% rare processes with high precision on simulated attacks.
- Integrating VirusTotal enrichment with a self-training risk scoring model, achieving a +20% PR-AUC lift compared to VT-only thresholds.
- Engineering 15+ process and network features (path, signer, parent/child, prevalence, connections) to improve detection accuracy to 95%+ on test scenarios.
- Developing a Streamlit dashboard with JSON/CSV export, enabling live triage of 50+ processes per cycle with clear explanations.

Simple SIEM for Home Network (*In Progress*)

- Designing a home network SIEM solution using Datadog for centralized log collection, monitoring, and real-time alerting.
- Configuring Datadog SIEM to ingest 500+ logs per second from network devices, flagging critical security anomalies daily using customized threat detection rules.
- Developing custom dashboards for visualizing network events, monitoring device behavior, and detecting suspicious activities.

Cybersecurity Policy Development for ICS-Based Critical Infrastructure (*Jun 2025*)

- Created a comprehensive Information Security Handbook for Industrial Control Systems (ICS) in the dam sector, incorporating policies for Acceptable Use, Asset Management, Backup & Recovery, BYOD, Incident Response, and Information Disposal.
- Aligned policies with NIST CSF, NIST 800-82, NIST 800-61, NIST 800-88, ISO 27001, GDPR, and HIPAA to enhance security posture and regulatory compliance.
- Mapped technical and behavioral controls to NIST 800-53 to improve ICS security and resilience.

Local Risk Analyzer – Windows Vulnerability Detection Tool (*Mar 2025*)

- Developed a Python-based CLI tool to assess system vulnerabilities, with the NVD CVE API, CPE matching, CVE and CVSS scoring for accurate risk evaluation.
- Automated security report generation in JSON, TXT, and HTML formats which aided in detecting 100+ vulnerabilities weekly and improved accuracy of risk assessment reports.

Digital Signature Tool (*Dec 2021*)

- Implemented RSA, DSA, and ECC algorithms to compare digital signature speed, computational efficiency, and data integrity.
- Built software with Python Tkinter to demonstrate digital fingerprinting processes with 4 algorithms (RSA, DSA, ECC, ElGamal).
- Authored a thesis analyzing digital signatures and public key cryptography.

Publications

Shrestha, Y., Ansari, K., & Aksoy, A. (2025, May). Automated IoT Fingerprinting with LLMs: Harnessing Explainable AI and Artificial Bee Colony Optimization. In 2025, IEEE Security and Privacy Workshops (SPW) (pp. 184-190). IEEE.

DOI [10.1109/SPW67851.2025.00024](https://doi.org/10.1109/SPW67851.2025.00024)

Aksoy, A., Varma, S., Ansari, K., & Shrestha, Y. (2025, May). Automated Host Identification Using SSL/TLS Traffic with SHAP and Artificial Bee Colony. In 2025, IEEE Conference on Artificial Intelligence (CAI) (pp. 950-955). IEEE.

DOI [10.1109/CAI64502.2025.00167](https://doi.org/10.1109/CAI64502.2025.00167)
