Yaman Shrestha
121 E Hunt Ave, 64093, MO
Phone: +1-(816)-200-4388
Email: yamanshrestha08@gmail.com, yxs33220@ucmo.edu
Social: linkedin.com/yaman-shrestha, github.com/yamanshrestha

Skills and Technical Background

- Centralized threat intelligence feeds into **Datadog SIEM, ELK Stack, and Splunk** to aggregate logs, conduct threat hunting, triage incidents, and support SOC operations.
- Applied **Threat Intelligence** methodologies to identify **Indicators of Compromise** (IOCs), analyze attack vectors, and support threat detection within SOC environments.
- Leveraged the **Cyber Kill Chain** and **MITRE ATT&CK** frameworks to analyze adversary tactics, techniques, and procedures (TTPs), improving incident response and threat mitigation strategies.
- Conducted real-time packet analysis and traffic monitoring using **Wireshark, Tcpdump, and Tshark**, enhancing incident detection and forensic investigation capabilities.
- Created an **Incident Response Plan** aligned with **NIST SP 800-61r2**, incorporating the **PICERL** model to strengthen detection, containment, and recovery processes for Dam sector.
- Trained **LLMs (Large Language Models)** to enhance incident classification and IoT device fingerprinting, achieving **98%** detection accuracy and advancing SOC threat detection capabilities.
- **Published** a paper "Automated IoT fingerprinting with LLMs: Harnessing explainable AI and Artificial Bee Colony Optimization" at *IEEE/ACM Workshop 2025. DOI: 10.1109/SPW67851.2025.00024*
- **Co-authored** a paper "Automated host identification using SSL/TLS traffic with SHAP and Artificial Bee Colony" at *IEEE Conference on Artificial Intelligence 2025. DOI: 10.1109/CAI64502.2025.00167*
- Completed advanced network security labs using **Python, Scapy, raw sockets**, and **packet manipulation** to implement **packet sniffing, spoofing, ARP/DNS attacks**, and traffic analysis.
- Completed **CCNA (Cisco Certified Network Associate)** course covering **Access Controls**, **VLANs, subnetting, CIDR, routing protocols (RIP, OSPF, EIGRP), ACLs, NAT, VPNs, SSL/TLS tunneling, IPv4**, and network security fundamentals.
- Configured hybrid cloud environments including **AWS EC2, Azure, DigitalOcean, and Akamai**, applying IAM controls, network segmentation, and continuous monitoring.
- Designed **Python** based automation scripts for **vulnerability detection**, **system hardening**.
- Integrated security best practices across projects by leveraging **MITRE ATT&CK, OWASP Top 10**, and threat modeling practices across projects.
- Led cross functional team of UI/UX, Frontend, Backend and DevOps of **15** members, managing secure project execution and aligning deliverables with client requirements, secure development.
- Written **policies, procedures, standards and guidelines,** for **Industrial Control Systems (ICS)** in dam sector aligned with **NIST CSF, NIST 800-53 controls** to enhance data protection, system resilience, and regulatory compliance for Dams and Health Sector.
- Completed **over 200 CAIQ, SIG** questionnaires, and regulatory frameworks to streamline third-party risk management and compliance reporting.
- Performed organizational **SWOT** analysis to evaluate cyber risks, identify security gaps, and inform strategic improvements.
- Collaborated within **Agile** and **Waterfall** environments to drive security initiatives across the software development lifecycle (SDLC).

Certifications

Currently Hold	**Pursing**
CompTIA Security+	Certified Ethical Hacker (CEH)
Certified in Cybersecurity (CC) - $(ISC)^2$	SOC Analyst
TCP/IP and Advanced Topics	CISA
ICSI CNSS Certified Network Security Specialist	
Learning Cloud Computing: Core Concepts	

Education

University of Central Missouri, **Lee's Summit, MO**
MS in Cybersecurity and Information Assurance Jan. 2024 – Present
Pursuing MS with a thesis option and completed advanced coursework in Ethical Hacking, Computer Forensics, Threat Intelligence, Cryptography, Advanced Networking, and Cyber Policy & Risk Management, applying theoretical knowledge to practical security projects and research initiatives.

Islington College (London Metropolitan University), **Kathmandu, Nepal**
BSc. (Hons) Computer Networking & IT Security *Aug 2018 – Dec 2021*
Achieved a strong technical foundation in CCNA Networking, Information Systems, Digital Crime Investigation, and Communication Engineering, focusing on network architecture, secure system design, and core cybersecurity concepts.

Work History

Graduate Research Assistant
University of Central Missouri – Warrensburg, MO *Aug 2024 – Present*

- Conducted in-depth research on network security, including TCP/IP packet analysis, IoT fingerprinting, incident detection techniques aligned with SOC practices.
- Fine-tuned LLaMA 2 7b and LLaMA 3 8b models with IoT and incident datasets for security use cases.
- Apply Explainable AI (XAI) and ABC Optimization to streamline security data analysis, reducing feature sets by 75% while maintaining high detection accuracy up to 98%.
- Evaluated performance comparison with Deep Learning models proving 17% better results with LLMs.

Team Lead
Syvar Technology Pvt. Ltd. – Lalitpur, Nepal *Apr 2022 – Dec 2023*

- Supervised a cross-functional team (15 members) to deliver seven security-focused projects on time and within budget.
- Designed and delivered internal training on security policies, incident response, and secure coding practices, enhancing team awareness.
- Supervised project execution, aligning security controls with company risk management objectives.

Security Research Analyst (GRC)
SecurityPal Inc. – Baluwatar, Nepal *May 2021 – Mar 2022*

- Conducted over 200 third-party risk assessments 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

Simple SIEM for Home Network *(In Progress)*

- Design a home network SIEM solution using Datadog for centralized log collection, monitoring, and real-time alerting.
- Configure Datadog SIEM to ingest 500+ logs per second from network devices, flagging critical security anomalies daily using customized threat detection rules.
- Develop 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.