SUNIL TIWARI

bishwast77@gmail.com
(318) 680-6123
Spanish Fork, UT

Summary

Cybersecurity Engineer & SOC Analyst Specialized in **Security Orchestration, Automation, and Response (SOAR)** and Event-Driven Architectures. Proven experience building autonomous incident response systems on **NVIDIA DGX (ARM64)** hardware, ensuring 100% data sovereignty with local LLM inference. Expert in **Wazuh SIEM**, **Python automation**, and **NIST 800-53** governance frameworks. Passionate about bridging the gap between detection and response through "Human-in-the-Loop" AI systems.

Core Blue Team Skills:

Security Operations: Wazuh SIEM, SOAR, Threat Hunting, MITRE ATT&CK, NIST 800-53, Incident Response (IR).
AI & Automation: Local LLMs (Llama 3.2), Ollama, CrewAI, LangChain, RAG (Retrieval-Augmented Generation).
Engineering: Python (Event-Driven), Streamlit (Dashboarding), NVIDIA DGX/Jetson (ARM64 Optimization), Docker, Linux (Ubuntu).

Portfolio

- GitHub Link: https://github.com/bishwast
- Portfolio Website: https://bishwast.github.io/
- LinkedIn: https://www.linkedin.com/in/suniltiwaricyber/
- **USA Permanent Resident**

SECURITY ENGINEERING PROJECTS:

Autonomous Agentic SOC on NVIDIA DGX | Dec 2025 – Present Built an end-to-end, event-driven SOC platform that autonomously detects, investigates, and responds to live cyber threats using local AI.

- Architected a real-time "Nervous System" bridge in Python that monitors Wazuh SIEM logs and triggers AI agents within <10 milliseconds of a high-severity alert.
- Engineered a multi-agent AI crew (using Llama 3.2 and CrewAI) to perform autonomous Threat Intelligence enrichment (AbuseIPDB) and risk assessment, reducing triage time by 95%.
- Developed a custom Analyst Console (Streamlit) to implement "Human-in-the-Loop" governance, ensuring all automated firewall blocks comply with NIST 800-53 authorization standards.
- Optimized the entire inference stack for ARM64/AARCH64 architecture on NVIDIA DGX, achieving 100% data sovereignty by eliminating cloud API dependencies.
- Validated system resilience against real-world adversary emulation (MITRE T1110 Brute Force) using Hydra, confirming zero-latency detection and response.

Enterprise SIEM & Attack Simulation | Home Lab | Nov 2025 – Present

- SIEM Deployment: deployed Splunk Enterprise on Linux to monitor authentication logs and system metrics.
- Attack Simulation: Scripted Bash-based attacks (Brute Force) to validate threshold-based alerting rules.
- Threat Visualization: Created executive dashboards to map threat origins and analyze attack volume.

Independent Security Researcher & Technical Consultant | Remote | Jan 2023 – May 2024

- Dedicated period of advanced professional development focused on Cloud Security, Python Automation, and SOC architecture.
- Designed and deployed home-lab environments mimicking enterprise networks to simulate Red/Blue team scenarios (Splunk, Wazuh).
- Developed Python scripts to automate log parsing and API interactions, building the foundation for autonomous SOC projects.
- Obtained CompTIA CySA+ certification and advanced proficiency in Linux administration and Docker containerization.

Full-Time Student (BS in IT Network Security) | Utah Valley University | Orem, UT

Sept 2020 – Dec 2022

- Completed intensive coursework in Network Defense, Cryptography, and Scripting for Security (Python/Bash).
- **Capstone Project**: Designed a secure campus network architecture, including comprehensive Business Continuity and Disaster Recovery plans.

Professional Experience

Compliance & Operations Specialist | Intermountain Health • American Fork, UT 05/2024 - 08/2024

1. Enforced strict access controls and HIPAA compliance for sensitive Patient Health Information (PHI).
2. Audited EHR access logs to identify potential unauthorized access or policy violations.

IT Operations Manager | Karuwaa Express • Sandy, UT 08/2024 - 04/2025

1. Developed a Risk Treatment Plan for high-risk assets and implemented RBAC to enforce least privilege.
2. Delivered Staff Security Awareness Training on Phishing/Malware, achieving a 0% click rate on simulations.

Partner Support Specialist | Walmart eCommerce | Draper, UT (Remote) Sep 2020 – Sep 2021

1. Managed complex enterprise workflows across Salesforce CRM instances, diagnosing and resolving high-priority partner issues.
2. Drove process optimization initiatives that resulted in a 20% improvement in team productivity metrics and case resolution times.
3. Collaborated with cross-functional technical teams to troubleshoot system integration errors and ensure platform stability.

Customer Service Representative | Vivint Smart Home | Lindon, UT (Hybrid) Jul 2019 – Sep 2020

4. Provided Tier-1/Tier-2 technical support, diagnosing and resolving complex device connectivity and data quality issues.
5. Authored internal technical documentation and knowledge base articles to streamline troubleshooting workflows.
6. Mentored and trained new hires on remote troubleshooting protocols, improving team response times and resolution metrics.

IT Support Help Desk | CenturyLink • Monroe, LA 01/2019 - 05/2019

1. Managed Active Directory for 100+ endpoints, resolving ACL violations and enforcing Group Policy objects.

2. Provided remote technical support for VPN/Citrix infrastructure using PowerShell for troubleshooting.

EDUCATION & CERTIFICATIONS

1. Master of Science in Cybersecurity Management | University of Utah | Expected July 2026
2. Bachelor of Science in IT Network Security | Utah Valley University | Dec 2022
3. CompTIA Cybersecurity Analyst (CySA+) | Code: N36L2QGYX1VQ52KJ