Sunil Tiwari

suniltiwari.me | bishwast77@gmail.com | (318) 680-6123 | GitHub | LinkedIn

EXPERIENCE

Karuwaa Express | IT Operations Manager — Sandy, UT
Aug 2024 – Apr 2025

- Executed a Formal Risk Treatment Plan for high-risk assets and implemented Role-Based Access Control (RBAC).
- Designed mandatory Staff Security Awareness Training, achieving a 0% phishing click rate.
- Mitigated internal fraud through least privilege enforcement and comprehensive security monitoring.

Intermountain Health | Patient Access (Identity & Compliance) — UT
May 2024 – Aug 2024

- Enforced HIPAA and PCI-DSS compliance protocols during patient intake processes.
- Mitigated identity theft risks through rigorous PII verification and insurance validation.

Walmart eCommerce | Partner Support Specialist — Remote
Sep 2020 – Sep 2021

- Managed enterprise workflows across Salesforce instances, resolving high-priority technical and partner issues.
- Drove process optimization resulting in a 20% improvement in overall team productivity.

CenturyLink | IT Support Help Desk — Monroe, LA
Jan 2019 – May 2019

- Managed Active Directory for 100+ endpoints, enforcing GPOs and resolving Access Control List (ACL) violations.
- Provided remote systems support and integration troubleshooting for VPN and Citrix infrastructure using PowerShell.

ENGINEERING PROJECTS

Hybrid-LLM Autonomous SOC & Active Defense Framework
Security Automation Architect | Dec 2025 – Current

- Architected a Hybrid-LLM Autonomous SOC utilizing the CrewAI framework to orchestrate local edge models (Llama 3.2) and cloud intelligence (GPT-4o) for zero-intervention threat triage and incident response.
- Integrated isolated Docker honeypots with a custom FastAPI backend, engineering regex-driven Python telemetry bridges to dynamically extract ephemeral attacker IPs and ingest raw log data into the cognitive pipeline.
- Engineered a deterministic Active Defense Governance Layer in Python to intercept and audit AI-generated actuation commands, enforcing strict infrastructure IP whitelisting to prevent AI hallucinations and host-level Self-Denial-of-Service (DoS).
- **Multi-Tenant Integration:** Successfully ported the Agentic engine to defend a simulated Web Application stack; reconfigured RAG playbooks and decoders to handle Layer 7 telemetry and triage web-specific vulnerabilities (SQLi/RCE).
- Achieved autonomous threat containment by programmatically actuating dynamic `iptables` drop rules against validated malicious endpoints, preserving core DNS and network routing integrity.

EDUCATION

University of Utah
MS Cybersecurity Management
Exp July 2026 | Salt Lake City, UT

- **Specialization:** Agentic AI in SecOps

Utah Valley University
BS IT Network Security
Dec 2022 | Orem, UT

SKILLS

Agentic AI & Orchestration
CrewAI • LangChain • LLM SecOps • Prompt Engineering • Llama 3.2 • Ollama • RAG

Security Engineering
Autonomous Incident Response • SIEM (Splunk/Wazuh) • Forensic Triage • MITRE ATT&CK • Linux Kernel Networking • Vulnerability Management

Infrastructure
NVIDIA DGX (ARM64) • Python (FastAPI) • Docker • Azure • Active Directory • PowerShell

CERTIFICATIONS

CompTIA CySA+
Microsoft AZ-500 *(MSCM Capstone Candidate)*