

SUNIL TIWARI

bishwast77@gmail.com
3186806123
Spanish Fork, UT

Summary

CySA+ certified Cybersecurity Professional and MSCM candidate with a specialized focus on AI-driven SOC operations and GRC. Proven expertise in engineering end-to-end security pipelines, most recently deploying a native Wazuh SIEM on NVIDIA DGX Spark (ARM64) integrated with local Llama 3.2 for automated Tier-1 threat analysis and autonomous remediation via Python-based active response.

Demonstrated track record in high-compliance environments, including enforcing HIPAA and PII data handling standards at Intermountain Health and developing formal Risk Treatment Plans and RBAC frameworks at Karuwaa Express. Proficient in managing complex technical controls including Palo Alto Firewalls, Splunk Enterprise, and Linux Netfilter (iptables) to mitigate alert fatigue and harden organizational security postures. [USA Permanent Resident](#).

Core Blue Team Skills: SIEM Administration (Splunk), Threat Detection & Analysis, Access Control Management (IAM), Network Security, Log Analysis.

Certifications: CompTIA Cybersecurity Analyst (CySA+) Certified.

Portfolio

GitHub Link: <https://github.com/bishwast>

Portfolio Website: <https://bishwast.github.io/>

LinkedIn: <https://www.linkedin.com/in/suniltiwaricyber/>

Experience

SOC Analyst

Independent Projects Cybersecurity Analyst (Home Lab & Simulation) • Spanish Fork, UT 11/2025 - Present Implemented end-to-end

1. SIEM Implementation: Designed and deployed a Security Operations Center pipeline using Splunk Enterprise on a virtualized Linux server.
2. Log Analysis & Regex: Developed custom SPL queries and Regex for parsing unstructured authentication logs to facilitate deep-dive threat analysis.
3. Attack Simulation: Scripted a Bash-based attack simulator to validate threshold-based alerts for common attack patterns, ensuring alert reliability.
4. System Optimization: Resolved complex data ingestion failures using CLI-based debugging and configuration for a 100% operational log pipeline.
5. Threat Visualization: Created an executive dashboard to visualize attack volume and map threat origins, improving incident reporting efficiency.

Front-line Operations & Compliance

Intermountain Health • American Fork, UT 05/2024 - 08/2025

1. Implemented and enforced strict access controls to protect patient information
2. Ensured compliance with HIPAA regulations at all times
3. Conducted thorough verification of Personally Identifiable Information (PII) for patient intake
Maintained accuracy and confidentiality of patient records in the EHR system
4. Collaborated with team members to uphold security protocols

5. Regularly audited and monitored access to patient records for potential breaches

IT Operations Manager

Karuwaa Express • Sandy, UT 08/2024 - 04/2025

1. Developed and executed a Formal Risk Treatment Plan for high-risk assets
2. Implemented Role-Based Access Control (RBAC) to enforce least privilege
3. Mitigated internal fraud risk through effective risk management strategies
4. Designed and delivered mandatory Staff Security Awareness Training on Phishing/Malware
5. Achieved a 0% detection rate for phishing attempts over a seven-month period
6. Enhanced organizational security measures through proactive risk mitigation efforts

IT Support Help Desk

CenturyLink • Monroe, LA 01/2019 - 05/2019

1. Enforced security policies using the Group Policy Management Console to ensure system compliance and security baselines across the corporate network
2. Provided remote technical support for critical VPN/Citrix issues, utilizing PowerShell and Event Viewer for incident resolution and advanced troubleshooting
3. Managed Active Directory, resolving ACL violations and performing high-security functions such as password resets for over 100+ endpoints
4. Implemented access control protocols to reinforce system security
5. Conducted incident triage to address and resolve technical issues promptly
6. Utilized IAM operations to maintain system integrity and security compliance

Skills

Category, Skills, Security Operations Center (SOC), SIEM (Splunk Enterprise),, Security, Operations, Log Aggregation, Threat Detection, Vulnerability Management,, Incident Response, Network &, Perimeter, Firewalls (Palo Alto Networks), Group Policy Management,, Access Control, (IAM), Active Directory, Access Control Management (IAM), Role-, Based Access Control (RBAC), Scripting & OS, HIPAA/PHI Data Handling, PII Data Handling, Risk Assessment,, Compliance/GRC, Security Policy Implementation, Linux, Virtualization

Education

Masters of Science in Cybersecurity Management

- University of Utah - David Eccles School of Business • Salt Lake City, UT 07/2026

Bachelors of Science in IT Network Security

- Utah Valley University • Orem, UT 12/2022

Certification:

Comptia CySa+ N36L2QGYX1VQ52KJ

Verification Link: <https://cp.certmetrics.com/comptia/en/public/verify/credential>