SUNIL TIWARI

bishwast77@gmail.com
3186806123
Spanish Fork, UT

Summary

Highly focused cybersecurity professional specializing in **Security Operations Center (SOC) methodologies** and **Governance, Risk, and Compliance (GRC)**. MSCM candidate (Expected Dec 2026) with practical experience in SIEM implementation, threat detection, access control, and network security. USA Permanent Resident (No Sponsorship Required).

Dedicated to applying technical controls (Palo Alto Firewalls, Python, Splunk) to maintain a robust security posture and achieve compliance baselines (HIPAA, PII Data Handling). Seeking hands-on **SOC Analyst, Security Monitoring, or Incident Response** roles.

- **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/splunk-siem-lab

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

Experience

SOC Analyst

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

- Implemented end-to-end SIEM solution for threat detection
- Designed and deployed Security Operations Center pipeline using Splunk Enterprise on virtualized Linux server
- Developed custom SPL queries and Regex for parsing unstructured authentication logs for analysis
- Scripted a Bash-based attack simulator to validate threshold-based alerts for common attack patterns
- Resolved complex data ingestion failures using CLI-based debugging and configuration
- Created executive dashboard to visualize attack volume and map threat origins

Front-line Operations & Compliance

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

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

IT Operations Manager

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

- Developed and executed a Formal Risk Treatment Plan for high-risk assets
- Implemented Role-Based Access Control (RBAC) to enforce least privilege
- Mitigated internal fraud risk through effective risk management strategies
- Designed and delivered mandatory Staff Security Awareness Training on Phishing/Malware
- Achieved a 0% detection rate for phishing attempts over a seven-month period

- Enhanced organizational security measures through proactive risk mitigation efforts

IT Support Help Desk

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

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

Cybersecurity Management

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

IT Network Security

Utah Valley University • Orem, UT 12/2022

Certificates

CompTIA CySA+