DHRUV SRIVASTAVA

official.sridhruv@gmail.com | LinkedIn | GitHub

PROFESSIONAL SUMMARY

CompTIA Security+ (SY0-701) certified cybersecurity professional and 4th-year B.Tech Computer Science Engineering student with hands-on experience in **SIEM log analysis, threat detection, incident response, and security operations.** Proficient in Splunk Enterprise for real-time security monitoring, alert configuration, and log correlation. Knowledgeable in IAM, network security, cryptography, vulnerability assessment, and security frameworks including NIST and MITRE ATT&CK. Seeking an entry-level Cybersecurity Analyst / SOC Analyst role to apply threat identification and security monitoring skills in a production environment.

TECHNICAL SKILLS

Security Tools & SIEM: Splunk Enterprise, Log Analysis, Alert Configuration, Dashboard Creation, Security Information and Event Management (SIEM), IDS/IPS Concepts, Wireshark (Foundational)

Cybersecurity Domains: Threat Detection, Incident Response, Vulnerability Assessment, SOC Operations, Network Security, Identity and Access Management (IAM), Cryptography, Endpoint Security, Security Operations, Risk Assessment

Frameworks & Standards: NIST Cybersecurity Framework, MITRE ATT&CK, CIA Triad, SPF/DKIM/DMARC, OWASP Top 10

Programming & Scripting: Python, C, Bash Scripting (Foundational), Regular Expressions

Operating Systems & Platforms: Linux (Ubuntu, Kali Linux), Windows Security Tools, TryHackMe Labs, Command Line Interface (CLI)

CERTIFICATIONS

CompTIA Security+ (SY0-701) – CompTIA (Active)

Certified in Cybersecurity (CC) – ISC2

Cyber Security 101 Pathway – TryHackMe

PROFESSIONAL EXPERIENCE

Cybersecurity Intern *Sept 2025 – Dec 2025*

Dhanamitra Infotech LLP *Delhi NCR, India*

- Monitored and triaged 50+ daily security alerts using Splunk SIEM, identifying potential threats, suspicious IP activity, and anomalous user behavior across enterprise network environments
- Performed log analysis and event correlation in Splunk to detect failed login attempts, brute-force patterns, and unauthorized access, escalating high-priority incidents to senior analysts
- Assisted in system hardening initiatives including firewall rule reviews, access control audits, and baseline configuration checks aligned with security best practices
- Documented security incidents and remediation steps in technical reports, contributing to improved incident response workflows and SOC documentation standards

Cybersecurity Intern *July 2025 – Aug 2025*

CodeCraft Infotech *Delhi NCR, India*

- Studied and implemented classical cryptography techniques including Caesar Cipher, substitution cipher, and symmetric encryption/decryption methods to understand foundational cryptographic principles
- Documented attack vectors, threat methodologies, and remediation strategies in structured technical reports used for internal knowledge base development
- Researched common vulnerability types and attack surfaces, gaining foundational knowledge of penetration testing concepts and ethical hacking methodologies

CYBERSECURITY PROJECTS

SIEM Log Analysis – Threat Detection with Splunk Enterprise

- Deployed Splunk Enterprise in a lab environment to ingest, parse, and analyze security logs from multiple sources including authentication logs, firewall logs, and system event logs
- Created custom Splunk queries (SPL) and correlation rules to detect failed login attempts, brute-force attacks, and suspicious IP activity in real time
- Built interactive Splunk dashboards and configured automated alerts for high-severity security events, reducing mean time to detect (MTTD) for simulated threats

Phishing Email Detection System

- Developed a phishing email detection system using Python to analyze email headers, embedded URLs, and message body content for identifying malicious patterns and social engineering indicators
- Applied SPF, DKIM, and DMARC validation techniques to authenticate email sources and flag spoofed sender addresses, improving threat identification accuracy
- Integrated rule-based and machine learning classification techniques to categorize emails as legitimate, suspicious, or malicious with measurable detection rates

EDUCATION

ABES Institute of Technology (AKTU) *Aug 2022 – Expected Aug 2026*
Bachelor of Technology (B.Tech) in Computer Science Engineering | Ghaziabad, India

SR International School *April 2021 – March 2022*
Intermediate (PCM) – Percentage: 88.4% | Bareilly, UP

Bishop Conrad School *April 2019 – March 2020*
High School – Percentage: 79% | Bareilly, UP