Sunny Dev

SOC Analyst

9389413970 | sunnydev0411@gmail.com | Dehradun, Uttarakhand, India | LinkedIn | GitHub

SUMMARY

Final-year B.Tech CSE student with a strong foundation in cybersecurity. Skilled in monitoring, log analysis, and threat detection. Proficient in network security, vulnerability assessment, and security frameworks such as MITRE ATT&CK and the Cyber Kill Chain. Passionate about securing digital infrastructure, proactively mitigating cyber threats, and strengthening organizational security.

EXPERIENCE

Cybersecurity Analyst Job Simulation, TATA, Remote
- Successfully completed a **Cybersecurity Analyst Job Simulation**, gaining hands-on experience in key cybersecurity concepts and practices.
- Demonstrated proficiency in **Identity and Access Management (IAM)**, including fundamentals and strategy assessment.

EDUCATION

DIT University, Dehradun, India - *B.Tech CSE , - GPA: 7.99*   **2021 - Present**
PNF Public School , Pithoragarh, India - *Secondary Education, - GPA: 7.08*   **2020 - 2021**

CERTIFICATIONS

Digital Forensics Essentials

Google Cybersecurity

SOC Level 1

Cryptographic Hash and Integrity Protection

PROJECTS

Remote Scheduled Backup, Link
- Designed and developed a **Remote Scheduled Backup system** to automate secure data backups across distributed environments.
- Integrated **scheduling functionality** to enable automatic backups at user-defined intervals, optimizing operational efficiency.

Resource monitoring Script, Link
- Developed a **bash script** to monitor system resource utilization, ensuring optimal performance and early detection of potential issues.
- Utilized commands like `free`, `df`, and `awk` to extract and process system metrics efficiently.

Log File Analyzer, Link
- **Developed a Python-based log analysis tool** to parse and analyze web server logs, extracting key metrics such as IP addresses, request types, and response statuses.
- **Demonstrated strong understanding of web server log formats**, HTTP methods, and status codes for effective analysis and monitoring.

Phishing Email Detector, Link
- Developed a Python-based tool to detect and analyze phishing emails by examining email headers, content, and embedded URLs.
- Provided detailed analysis reports highlighting suspicious elements in the emails.

SKILLS

Languages	:	Bash Scripting, Python, SQL, Java
Frameworks	:	Cyber Kill Chain, OWASP, CIS Controls, MITRE ATT&CK, Incident Response, NIST Cybersecurity Framework
Tools	:	Linux, Nmap, Wireshark, Tcpdump, Snort, Wazuh, Autopsy
Threat Intelligence & Analysis	:	Cyber Threat Intelligence, Phishing Email Analysis, Malicious Document Analysis, Malware Analysis, Log Analysis

EXTRA

Basketball player
- Represented state and university-level basketball teams, demonstrating strong **teamwork, leadership, and strategic decision-making** under pressure.