SACHIN GAUTAM

Cybersecurity Student & Associate SOC Analyst

sachingautam0b@gmail.com | Kalanki, Kathmandu | sachin01.com.np | LinkedIn | GitHub | Medium

PROFESSIONAL SUMMARY

Final-year BScIT student and Associate SOC Analyst with real-world experience in security monitoring, incident response, and threat detection. Hands-on with SIEM platforms in live SOC environments, with a track record of improving detection quality and supporting security operations across multiple client environments. Passionate about cybersecurity, continuous learning, and making security operations more effective.

PROFESSIONAL EXPERIENCE

Associate SOC Analyst

Aug 2025 Mar 2026

Cryptogen Nepal Pvt. Ltd. Kathmandu, Nepal

- Monitored and triaged security alerts across multiple client environments using SIEM platforms on a 24/7 basis.
- Built and tuned detection rules, alerts, and dashboards to improve the quality and accuracy of security event detection.
- Validated log ingestion and coverage from systems, applications, and endpoints to ensure complete visibility.
- Investigated security incidents, collected evidence, and coordinated containment and remediation with relevant teams.
- Conducted proactive threat hunting using the MITRE ATT&CK framework to identify threats before they caused impact.
- Documented investigation findings and contributed to improving SOC playbooks and workflows.
- Delivered knowledge transfer sessions to new analysts to standardise team processes and improve overall capacity.
- Prepared clear security reports for stakeholders, translating technical findings into practical recommendations.

SOC Analyst Intern

Jun 2025 Jul 2025

Cryptogen Nepal Pvt. Ltd. Kathmandu, Nepal

- Supported real-time SIEM monitoring and alert analysis across multiple client environments.
- Investigated phishing campaigns, suspicious domains, and IP addresses using threat intelligence tools.
- Performed log correlation and incident triage to identify and help neutralise potential threats.
- Contributed to threat hunting and digital forensic investigations as part of the SOC team.

Cybersecurity Intern

Apr 2025 May 2025

Hack Secure Remote, India

- Conducted vulnerability scanning across lab network environments using Nmap and Metasploit.
- Participated in simulated penetration testing exercises to identify gaps in security controls.
- Wrote technical reports summarising vulnerabilities, their potential impact, and remediation steps.

TECHNICAL PROJECTS

Malicious IP Analyzer
A web application that checks multiple IP addresses for malicious activity using the AbuseIPDB API, with WHOIS lookup for additional context. Built to speed up the IP investigation process during alert triage.

Face Recognition Attendance System
An attendance management system using real-time facial recognition. Includes user registration, automated attendance marking, and an admin panel for viewing records.

Secure App
A mobile security application with user authentication and IP geolocation mapping, designed to support security-related data management on mobile devices.

Rato Daku
A collaborative Android security testing tool that uses ADB to identify mobile vulnerabilities and security misconfigurations in Android devices.

Secure Password Manager
A browser-based password manager with secure credential storage and a clean, easy-to-use interface.

ACHIEVEMENTS AND CONTRIBUTIONS

- Identified and reported security vulnerabilities in a local web platform including unauthorised access and enumeration issues, with recommended fixes.
- Reported a fraudulent online scam to the Cyber Bureau, contributing to the apprehension of the individual responsible.
- Active contributor to a cybersecurity club focused on dark web monitoring, reporting data leaks, and identifying malicious online activity.
- Consistent participant in CTF competitions on TryHackMe and Blue Team Labs Online with top-tier rankings.

CERTIFICATIONS

Fortinet Certified Fundamentals Cybersecurity
Fortinet Jul 2025

Introduction to the Threat Landscape 3.0
Fortinet Jul 2025

AWS Cloud Quest: Cloud Practitioner
Amazon Web Services Feb 2025

Cyber Threat Management
Cisco Networking Academy Sep 2024

AWS Academy: Cloud Web Application Builder
Amazon Web Services Sep 2024

Introduction to Critical Infrastructure Protection
OPSWAT Academy 2024

Getting Started in Cybersecurity 3.0
Fortinet Jul 2025

Python Essentials 1
Cisco Networking Academy Mar 2025

Ethical Hacker
Cisco Networking Academy Sep 2024

Introduction to Cybersecurity
Cisco Networking Academy Nov 2024

ISO/IEC 27001:2022 Information Security Associate
SkillFront 2024

Introduction to Networking
HTB Academy 2024

EDUCATION

BSclT — Bachelor of Science in Information Technology Jul 2022 Present
Presidential Graduate School Baneshwor, Kathmandu

+2 Science (Computer Science) 2020 2022
Little Angels College Hattiban, Lalitpur

Secondary Education Examination (SEE) 2010 2020
Bardiya Academy and Polytechnic Research Centre Bardiya

TECHNICAL SKILLS

SIEM Platforms	LogPoint, FortiSIEM, LogRhythm
Security Ops	Alert Triage, Incident Response, Threat Hunting, Log Correlation, Detection Tuning
Frameworks	MITRE ATT&CK, Cyber Kill Chain
Tools	Kali Linux, Wireshark, Nmap, Metasploit, OSINT Tools, Digital Forensics, Active Directory
Networking	TCP/IP, DNS, HTTP, Packet Analysis
Programming	Python, Bash, JavaScript
Cloud	AWS (Cloud Practitioner, Web Application Builder)
Languages	Nepali (Native) Hindi (Fluent) English (Professional)