Aaditya Khati

SOC Manager

Aaditya.khati@hotmail.com
+977 980 1128469

About Me

SOC Team Lead with a demonstrated history of work in Offensive Security, Web Application Firewall Administration, Tuning and hands-on experience with Incident Response, Digital Forensics, threat intelligence. Practical experience with multi SIEM platforms regarding their deployment, administration and tuning. Have acquired multiple disciplines and accreditations in various domains of cyber security.

Work Experience

SOC Manager
Cryptogen Nepal Pvt Ltd.
Jun 2019 - Present

- Responsible for hiring and training SOC staff
- Formulate SOC stratigies
- Plan SOC architecture
- Manage Incident Handling procedures
- Primarily responsible for directing security event monitoring, management and response and cyber intelligence
- Ensuring incident identification, assessment, quantification, reporting, communication, mitigation and monitoring
- Responsible for overall use of resources and initiation of corrective action where required for Security Operations Center.
- Ensuring daily management, administration & maintenance of security devices to achieve operational effectiveness
- Ensuring threat management, threat modeling, identify threat vectors and develop use cases for security monitoring
- Creation of reports, dashboards, metrics for SOC operations
- Technical Presentations regarding various cyber security technologies
- Overview SOC and Vulnerability Management related projects for successful delivery

Aaditya.khati@hotmail.com
+977 980 1128469

Academic Tutor

Islington College, Kathmandu

Jan 2018 - Feb 2019 (1 years, 2 months)

Module:

- Networking Concepts

This module focuses on fundamental network terminology and concepts, e.g. protocols, Open System Interconnection (OSI) and TCP/IP models, Ethernet, Internet Protocol (IP) addressing, routing protocols and network devices, such as routers and switches. The module provides an opportunity for students to understand the interconnections of various networks and to be able to design and configure small-scaled networks given some typical (customers) requirements.

- Risk, Crisis and Security Management:

This module is in particular for those who wish to specialize in understanding, developing, and the application of IT security systems and measures in IT environments. It focuses on various aspects of security management and deals mainly with risk assessment, risk management, and standards and procedures. It provides students with an appreciation of the benefits security management provides within an information systems domain. This includes the choice and application of appropriate risk assessment and risk management techniques, coupled with an understanding of security standards and procedures.

Penetration Tester

Eminence Ways

Sep 2016 - Dec 2017 (1 Year, 4 months)

- Perform Vulnerability Assessment to determine threats and vulnerabilities on the client's network
- Perform Penetration Testing to accurately determine true risk of the threat
- Demonstrate Vulnerability Assessment and Penetration Testing using the basic Testing methodology- Reconnaissance, Scanning, Exploiting, Post Exploitation
- Technical and Executive Proof of Concept report per vulnerability

Aaditya.khati@hotmail.com
+977 980 1128469

Certification

LogRhythm Deployment Engineer | LogRhythm

LogRhythm Platform Administrator | LogRhythm

LogRhythm Support Engineer | LogRhythm

LogRhythm Security Analyst | LogRhythm

Certified in Cyber Security | ISC2

Certified Ethical Hacker (CEH) | EC-Council

Certified Payment Card Industry Security Implementer | SISA

Application Delivery Fundamentals 101 | F5

CCNA Certified Network Associate Cyber Ops | CISCO

Certified Sales Engineer | Tenable

PSE: Cortex Associate | Palo Alto Networks

PSE: Foundation | Palo Alto Networks

Trustee | Cyber Ark

Network Security Expert 3 | Fortinet

Aaditya.khati@hotmail.com
+977 980 1128469

Education

B.Sc. in Networking and IT Security
Islington College

+2, HSEB
Global College of Management

Achievements

Winner
LogRhythm: LogWars
2023

Recognized by Trip Advisor
Trip Advisor | Bug Bounty
2019
Recognized by Trip Advisor for discovering a security bug on their domain.

Recognized by Under Armour
Under Armour | Bug Bounty
2019
Recognized by Under Armour for discovering a security bug on their domain.

Recognized by Facebook
Facebook | Bug Bounty
2019
Recognized by Facebook for discovering a security bug on their domain.

Core Skill

- SIEM Implementation & Administration
- SOAR Implementation & Administration
- Digital Forensics
- Incident Response
- Vulnerability Assessment & Penetration Testing
- SOC Design & Implementation
- Security Consulting
- Cyber Security Training

Aaditya.khati@hotmail.com
+977 980 1128469

Associated Projects

Vulnerability Assessment & Penetration Testing

- Department of Road - Penetration Tester
- Mega Bank - Penetration Tester
- NCHL - Penetration Tester
- Everest Bank - Penetration Tester
- SmartChoice Technologies - Penetration Tester
- Prabhu Bank - Penetration Tester

SIEM and Security Monitoring (SOC)

- Kamana Bikas Bank Limited - Project Lead
- Nepal Telecom - Lead Deployment Engineer
- Nepal Police - Lead Deployment Engineer
- Nepal Investment Mega Bank - Project Lead
- Laxmi Sunrise Bank - Lead Deployment Engineer

Digital Forensics & Incident Response

- Mahalaxmi Bikas Bank Limited - Lead Investigator
- Sipradi Training - IR Analyst

Vulnerability Management

- NIC Asia Bank - Project Lead
- NMB Bank - Project Lead
- Nabil Bank - Project Lead
- Prabhu Bank - Project Lead
- Himalayan Bank - Project Lead

Aaditya.khati@hotmail.com
+977 980 1128469

Associated Projects

Web Application Firewall (WAF)

- Laxmi Bank - Implementation Engineer
- Nabil Bank - Implementation Engineer
- NMB Bank - Lead Implementation Engineer
- NCHL - Consultant
- One Bank Limited - Consultant

Hi, I'm Nirmal 👋

I help you Assess. Audit. Analyze. Advise.

About

I'm a cybersecurity enthusiast committed to strengthening digital ecosystems against evolving threats. With over a decade of experience, I co-founded Cryptogen Nepal where my team and I deliver cutting edge services in Offensive Security, Defensive Security and Governance, Risk & Compliance (GRC). Our pioneering work has been recognized with prestigious accolades including the ICT Startup Award & being listed among the Top 250 MSSPs worldwide, solidifying our role in shaping cybersecurity landscape.

Work Experience

Cryptogen Nepal Pvt. Ltd. Co-founder — 2019 - Present
Chief Technology Officer

Softwarica College of IT & E-commerce Part-time — 2022 - Present
Lecturer

Pentester Nepal Voluntarily — 2017 - Present
Community Leader

OWASP Nepal Voluntarily — 2021 - 2024
Community Leader

Eminence Ways Pvt. Ltd. Full-time — 2016 - 2019
Senior Security Researcher

Education

Lincoln University College — 2025 - 2027
Master of Computer Science

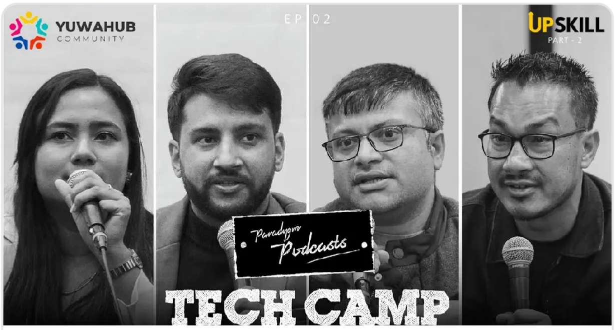
Languages

Nepali English Hindi

Media Coverages

Recent Media Coverages

Some of my recent notable appearances.



Upskill-Tech Camp 2025 | Tech Innovation, Networking, and Career Growth

March 8, 2025

Upskill-Tech Camp 2025 was a premier tech event held on March 8, 2025, at Herald International College. The event brought together industry experts, aspiring tech professionals, and leading companies to foster innovation, learning, and career development.

Paradygm Podcasts

Python Powered "Cyber Security" - Tools, Techniques, Exploitation and Automation | PyCon JP 2024

Sep 27, 2024 - Sep 29, 2024

Python has always been recognized as a language for web development, automation, analysis, and AI/ML. However, it has been crucial for cybersecurity experts as well. In my talk, I highlighted how Python is used in cybersecurity and the various areas where it plays a significant role.

PyCon JP

Episode 148: Cyber Security, World of Hacking, Cyber Safety - Sushant Pradhan Podcast

May 9, 2023

I was invited to the Sushant Pradhan podcast, where we discussed cybersecurity topics such as sidechannel vulnerabilities, IoT security, user awareness, zero-click attacks, MITM attacks, AI in cybersecurity, blockchain, scam calls, bug bounty hunting, and cyber safety practices for individuals and businesses.

Sushant Pradhan

राहदानी प्रणालीमा 'र्‍यान्समवेअर' आक्रमण 'शंकास्पद' - SAROKAR

Dec 11, 2024

The Department of Passport (Nepal) was compromised and scams and hacking were on the rise. To raise awareness, we were invited to Kantipur TV for the show called "Sarokar" where I, Bijay Limbu (VAIRAV Tech) and SP Deepak Awosti (Cyber Bureau) had an insightful session. I believe it had a significant impact on viewers.

Kantipur TV HD

Hacktivities

Notable Hacktivities

I find it fascinating to research and develop new things and engage in other cybersecurity activities. Here are some of my notable hacktivities.

March 20, 2025 - March 23, 2025

National Cyber Drill 2082 – Lead Trainer and Facilitator

Kathmandu, Nepal

CryptoGen Nepal had the privilege of supporting the National Cybersecurity Center (An entity under the Ministry of Communication and Information Technology) in organizing the annual "National Cyber Drill 2082" where more than 30 government agencies participated, represented by computer engineers, officers and directors. This 4 day event featured comprehensive training sessions covering a wide range of cybersecurity skills. I had the honor of serving as the Lead Trainer for this program and I am proud to have contributed to an initiative that helps strengthen and secure our nation’s digital infrastructure.

eKantipur LinkedIn

2024

First International Conference as a Speaker - PyCon JP 2024

Japan

I have always believed and still do that Python is one of the most suitable languages for cybersecurity as it is used everywhere from exploit development to automation. Since people generally don’t think about this aspect much, I always wanted to highlight its importance. Finally, I got the opportunity to do so at PyCon JP 2024 and I express my gratitude to PyCon JP for this oppurtunity.

PyCon JP

2021

Top 10 Ethical Hacker in The World by EC-Council

Worldwide

I was listed among the top 10 ethical hackers in the world by EC-Council, a renowned organization known for its prestigious certifications like Certified Ethical Hacker (CEH). This recognition was awarded in the second quarter of April 2021 by EC-Council itself.

EC-Council

2021

My first CVE was officially assigned "CVE-2021-3258"

Worldwide

Question2Answer.org is the developer of Q2A, a platform similar to WordPress but specifically designed for Question and Answer forums like Stack Overflow. In 2017, I discovered a stored XSS vulnerability that could lead to account takeover. The issue was promptly fixed by the development team. However, considering its global usage, I obtained a CVE for this vulnerability in 2021, marking my first CVE assignment.

NIST MITRE Youtube

June 6, 2019

Finding XSS on Samy Kamkar's Site

Worldwide

Samy Kamkar, a legendary figure in the world of security, has crafted his website in a way that makes it nearly impossible to even view the code, let alone find an XSS vulnerability. Yet, I managed to uncover one on his site, which felt like a huge achievement. Samy is a master in many areas of security, and finding a vulnerability on his site is something I will always cherish. He is the mastermind behind the MySpace XSS worm, the world's fastest-spreading JavaScript-based worm. The fact that I was able to find the same vulnerability on a legend's site and contribute to securing it makes this discovery feel like a milestone in my own journey.

Samy Kamkar Wikipedia

2017

Top 25 in YESWEHACK Platform

Worldwide

It was the first quarter of 2017 when one of Europe's earliest bug bounty platforms, BugBounty Factory (now called YesWeHack) had recently launched. I spent a significant amount of time on the platform and ranked among the Top 25 bug bounty hunters.

YEWWEHACK

Jan 21, 2017

1st Runner Up in HackBack CTF 2017

Nepal, Kathmandu University

HackBack, held as part of Kathmandu University's annual IT Meet in 2017 and organized by Rigo Technology, featured Nepal's first on-site CTF competition. I secured 1st Runner-Up in this prestigious event.

Certifications

That Define Me

I am passionate about continuous learning and earning certifications to stay ahead in my field. Among the 17+ professional certifications I have achieved, here are some of my recent and notable ones.

Jun 2025

Certified Multi-Cloud Blue Team Analyst

Cyber warfare Labs

Hands-on role in defending against advanced persistent threats across multi-cloud (AWS, Azure & GCP) environments, identifying vulnerabilities and strengthening cloud security posture through continuous monitoring and threat mitigation.

Apr 2025

Multi-Cloud Red Teaming Analyst

Cyber warfare Labs

Hands-on role in simulating advanced persistent threats across multi-cloud (AWS, Azure & GCP) environments, identifying vulnerabilities and improving cloud security posture.

Nov 2024

ISO/IEC 27001:2022 - Lead Auditor

International Organization for Standardization

Qualified to lead and conduct audits of Information Security Management Systems (ISMS) in compliance with the ISO/IEC 27001:2022 standard.

Jul 2022

DevSecOps - Introduction

AppSecEngineer

Introduced to the fundamentals of integrating security into DevOps pipelines using tools and practices like CI/CD security, IaC, and container hardening.

Mar 2021

Certified Ethical Hacker - Master

EC-Council

Certification showcasing proficiency in real-world ethical hacking techniques, including simulated attack scenarios.

Mar 2021

Certified Ethical Hacker - Practical

EC-Council

Performance based certification proving hands-on ability to identify and exploit vulnerabilities in a real-time environment.

Jul 2020

Certified Payment Card Industry Security Implementer

SISA Infosec

Specialized in implementing and maintaining PCI-DSS compliance for securing payment card data.

Jun 2020

Certified Ethical Hacker - ANSI

EC-Council

Internationally recognized certification in ethical hacking, covering penetration testing, network security, and system vulnerabilities.

Skills

Cybersecurity Consulting · Penetration Testing · Digital Forensics · Incident Response · Malware Analysis · SIEM Engineering · Security Awareness · Security Training · Security Research · Information System Audit · Security Strategy · Public Speaking · Leadership · Programming · SecDevOps · Docker

Contact

Need cybersecurity help?

Assess. Audit. Analyze. Advise.

whois@nirmaldahal.com.np