Nitish Kumar

Senior Analyst

ernitishjha30@gmail.com ✉

7488184058

New Delhi, India

linkedin.com/in/nitish-kumar-45787b1a6

github.com/nitishjha30

A results-oriented and highly skilled **SOC Analyst with 2+ years of experience** in **monitoring, detecting and responding to cybersecurity incidents using SIEM tools**. Skilled in incident triage, threat hunting, vulnerability management, risk assessments and implementing robust security measures with a strong focus on cloud security, network security and intrusion detection. Possessing a strong technical background, exceptional analytical skills and a proven track record of delivering effective **cybersecurity solutions.** I'm poised to apply my learning and gain further experience in research. Excited about the significant potential of being a part of your esteemed team, I believe my skillset can contribute effectively.

WORK EXPERIENCE

Senior Analyst

HCLTech

01/2024 - Present *Noida, India*

Achievements/Tasks

- Promoted as Senior Analyst in **January 2024.**
- Currently working for **4 clients 24x7** concurrently to maintain **Cloud Native & Network Security.**
- Monitor **security alerts and network traffic** for signs of potential threats or breaches & prioritize and remediate identified vulnerabilities to minimize the risk of exploitation & strategically handles SOC escalations.
- Experience with **Sentinel, ServiceNow Tasks, M365 Defender and other Azure Services.**
- Experience with **handling incidents** like IOC, Deployment, Malware, Phishing, Publicly Exposed Data, Threat Hunting & Azure Cloud related cases, Incident Audits, Fine-Tuning Alerts and Security Incident Documentation and Reporting.

Analyst

HCLTech

09/2022 - 12/2023 *Noida, India*

Achievements/Tasks

- Followed Incident Management and used to create SOP and Weekly Reports for the documentation and client calls.
- Tracked Incident Handling Playbooks, automation rules, analytical rules according to the process required.
- Released vulnerability advisories for CSFC to all the clients and management for path implementation

Web Development Intern

Mind IT Systems

01/2022 - 04/2022 *Delhi, India*

Design, develop, test, deploy, and maintained web applications

EDUCATION

B. Tech in Computer Science (Hons)

Dr. A. P. J. Abdul Kalam Technical University

08/2018 - 07/2022 *Lucknow, India*

Courses

- **84.2 %** in B. Tech

SKILLS

SOC · Azure Sentinel · M365 Defender · Azure Active Directory · SIEM · SOAR · Security Management · Email Security · Incident Response · Malware Analysis · Incidents Audits · Infrastructure Security · Threat Hunting · KQL · SQL · Internet Security · Azure Firewall · Data Analysis · Playbooks · SOP Creation · ServiceNow Incident Management · Computer Networks · MITRE ATT&CK Framework · Cybersecurity Analysis · CompTIA Security+ · HTML · C · Python · Linux · Data Structure

STRENGTHS AND EXPERTISE

Frameworks

- NIST , MITRE ATT&CK , ITILv4, PCI-DSS

SIEM

- Azure Sentinel , IBM QRadar

EDR/XDR

- Microsoft 365 Defender

Vulnerability Management

- M365 Defender, Tenable Nessus

Active Skills

- Incident Management, SOCv2 Lifecycle, Threat Hunting, Risk Assessment, Vulnerability Assessment, Email Security etc.

TRAININGS AND CERTIFICATES

- Microsoft Azure SC-200, SC-900, AZ-500, AZ-900, AI-900 Certified

- Google Cloud Professional Security Engineer Certified

- ITIL 4 Certified, CompTIA Security+ (Skillsoft)