NAVEEN KUMAR

Cyber Security Expert
7+ Years Exp

nav23nkumar@gmail.com | +971 559435547 | /in/nav2enkumar | hackernaveen.in

Energetic and passionate Ethical Hacker, Cyber Security Expert, Bug Bounty Hunter, & Trainer with strong proven experience in various branches of Cyber Security with the ability to deliver high-quality reporting on identified technical challenges and providing remediation guidelines for better security in the business landscape.

TECHNICAL CREDENTIALS

- Leadership & Mentorship
- Web App & Infra VAPT
- Red Teaming
- Security Monitoring
- Threat Hunting
- Scripting & Automation
- Incident Response
- Cloud Operations – AWS
- Cyber Forensics

TOOLS HANDS-ON

SIEM: Qradar, FortiSIEM, ELK, RSA Netwitness, Logrhythm, Splunk, Securonix
EDR: CrowdStrike, Sophos
NDR: DrakTrace
DLP: EndPoint Protector, Digital Guardian
Email Security: Microsoft Defender
Deep & Dark Net Monitoring: XVigil
Application Control: ThreatLocker
VMDR: Qualys
VAPT: Kali, Nessus, BurpSuite, ZAP, and more
Forensics: Wireshark, FastIR, FTK Imager
Ticketing: FreshWorks, Jira

WORK CREDENTIALS

AVRIOC TECHNOLOGIES
Sep 2024 to Present

Role: Cyber Security Engineer
Responsibilities:

- Leveraging SIEM and XDR solutions to monitor, detect, and respond reducing MTTR by 68%.
- Managing EDR to ensure endpoint protection, and unauthorised access control, investigate heuristic detections and mitigate threats.
- Utilizing NDR solution to analyze network traffic patterns and identify anomalies to proactively correlate and defend against sophisticated network attacks.
- Improved overall security posture by 45% by conducting timely VA and pushing patches.
- Leveraging DLP to prevent exfiltration of confidential data, while monitoring the dark and deep web for potential threats and compromised data, providing actionable intelligence to prevent data breaches.
- Managing endpoints from unauthorized access to software or privilege by extensive application control.
- Achieving security automation through generative AI to automate repeated daily/monthly tasks.

PRESIDIO
Jun 2023 to Aug 2024

Role: Technical Account Manager (Senior SOC Analyst)
Responsibilities:

- Client Relationship Management: Ensured client satisfaction by addressing security concerns.
- Incident Response Coordination: I led the incident response, working closely with the clients' SOC team to ensure timely and effective resolution of security incidents.
- Service Improvement Planning: Collaborated with the clients to identify areas for improvement in security services and develop plans to enhance SOC capabilities and processes.
- Technical Advisory: Offered expert advice on security technologies and best practices, helping clients make informed decisions about their security posture and investments.

- Compliance Support: Ensured that SOC services meet industry standards and regulatory requirements, assisting clients in achieving and maintaining compliance.

FST INFORMATION TECHNOLOGY PVT LTD — Jan 2022 to May 2023

Role: L2 SOC Engineer

Responsibilities:

- As a key engineer, built a Security Operation Centre from scratch for a client in Germany to become the leading MSSP in the global market and onboarded new clients for security monitoring.
- Solely responsible for SOC engineering, administration, and management for continuous monitoring.
- Led the team of L1 analysts on log monitoring, threat hunting & incident response.
- Created various SOPs for standard SOC procedures, operations, and executions.
- Created a new parser or fine-tuned existing log parsers.

SISA INFORMATION SECURITY PVT LTD — May 2019 to Dec 2021

Role: Incident Response/Handling Lead

Responsibilities:

- Led the team on incident handling & response and served as the associate lead for SIEM operations.
- Trained my team members on threat hunting for web application attacks with live attack simulation.
- Performed Web Application Penetration Testing on the in-house SIEM tool.
- Performed Red team activity and infrastructure VAPT during the cyber drill activities.

Role: Security Analyst

Responsibilities:

- Install & configure Logstash for grokking and structuring raw logs received from various devices.
- Deploy log forwarding agent in all the desktops, servers, firewalls & network devices.
- Composing custom groks and ECS-based groks for easy parsing of logs.

TEVEL CYBER CORPS PVT LTD — Nov 2018 to Apr 2019

Role: Information Security Analyst

Responsibilities:

- Created a deliberately vulnerable web application to train candidates on the latest trends and attacks of web application security.
- Conducted Static and Dynamic Application Security Testing on web applications.

REWARDS & RECOGNITIONS

- Reported multiple responsible disclosures related to web application and email security vulnerabilities.
- I received multiple spot awards in SISA for publishing technical blogs.
- Underwent & organized multiple ethical hacking workshops.
- I have trained 1000+ students and professionals on Cyber Security threats and prevention.

CERTIFICATION

Endpoint Detection & Response
Sophos Central Endpoint and Server Protection Certified Engineer v4.0 (ET15)

Security Information Event Management
RSA NetWitness Suite

ACADEMIC CREDENTIALS

M.Sc in Cyber Forensics & Information Security
University of Madras, Chennai, India.
Jan 2020 - Dec 2021

B.Tech in Information Technology
Meenakshi College of Engineering, Chennai, India.
Jun 2014 - May 2018

DECLARATION

I am confident that the information provided is accurate and complete.