NAVEEN KUMAR

Cyber Security Professional

nav23nkumar@gmail.com | +91 9677071653 | /in/nav2enkumar | hackernaveen.in

Energetic & passionate Ethical Hacker, Cyber Security Expert, Bug Bounty Hunter, & Trainer with great experience in various branches including Security Operation Centre, Web Application Penetration Testing, Cyber Forensics, & Network Security along with the ability to deliver high-quality reporting on technical challenges identified & providing remediation guidelines for better security in the business landscape.

TOOLS EXPLORED

- **SIEM:** Qradar, FortiSIEM, ELK Stack, RSA Netwitness, Logrhythm, Splunk
- **EDR:** Sophos, Trellix
- **Web App VAPT:** Burp Suite, ZAP, Nikto
- **Network VAPT:** Nessus, Kali, & its tools
- **Forensics:** Wireshark, FastIR, FTK Imager

TECHNICAL SKILLS

- Security Information Event Management
- Web App Dev, Host & VAPT
- Threat Hunting
- Cyber Forensics & Incident Response
- Network Security
- Cloud - AWS

EXPERIENCE

PRESIDIO

Jun 2023 to Present

Role: Technical Account Manager (Senior SOC Analyst)

Responsibilities:

- Primary TAM managing multiple clients, services management and their escalations.
- Leading L1 SOC analysts on Log analysis, threat hunting & incident response.
- Review the daily/weekly/monthly reports through daily/weekly/monthly client calls.
- Requirement analysis and monitoring status through daily, weekly & monthly calls with clients.
- Highly focused on red teaming for simulating real-time use cases for effective SOC monitoring.
- Creating and finetuning the SIEM rules for offences and reports.
- Mapping existing and new use cases with MITRE ATT&CK framework.
- Performing vulnerability analysis and penetration testing on internal applications.
- Proposed an idea to build an in-house security monitoring solution in the internal hackathon.

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.
- Highly responsible for SOC engineering, administration, and management for continuous monitoring.
- Leading a team of L1 analysts on log monitoring, threat hunting & incident response.
- Upgrading FortiSIEM in demo and production environments for each new version release.
- Test the new features or device integration in demo and production environments.
- Create various SOPs for standard SOC procedures, operations, and executions.
- Create alerts and correlation alerts to identify critical use cases and incidents.
- Create a runbook for all the existing and new security incidents.
- Perform manual attack simulation to test and validate use cases deployed.
- Create customer-specific, device-specific, and other custom dashboards and reports.
- Create a new parser or finetuning the existing log parsers.

SISA INFORMATION SECURITY PVT LTD **May 2019 to Dec 2021**

Role: Incident Response/Handling Lead

Responsibilities:

- I lead the team on incident handling & response and have been the associate lead for SIEM operations.
- I train team members on threat hunting and web application security with live attack simulation.
- Create threat dashboards for critical & medium incidents of Palo Alto, WAF, FortiGate & ASA firewalls.
- Create custom filters and conditions for quick identification of threats.
- Create alarm alerts and correlation alerts for all security incidents.
- Create shell script for elasticsearch shards allocation and data backup from the production environment.
- Performing vulnerability analysis and penetration testing on the in-house SIEM tool.
- Perform Red team activity and VAPT service for cyber drill activity.
- Perform vulnerability analysis scans on critical servers (PCI) and recommend patching.

Role: Security Analyst

Responsibilities:

- Deploy log forwarding agent in all the desktops, servers, firewalls & network devices.
- Install & configure Elasticsearch for data storage.
- Install & configure Logstash for grokking and structuring raw logs received from various devices.
- Composing custom groks and ECS-based groks for easy parsing of logs.
- Deploy different agents for forwarding other non-system logs.
- Test the in-house SIEM tool for any vulnerabilities and report them.
- Create use cases to enhance the existing features & incorporate the new features in the SIEM tool.
- Create various SOPs for deployment, monitoring, and threat hunting.

TEVEL CYBER CORPS PVT LTD **Nov 2018 to Apr 2019**

Role: Information Security Analyst

Responsibilities:

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

ACHIEVEMENTS

- Reported multiple responsible disclosures related to web application and email security.
- 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.
- I received numerous appreciation for reporting critical web app bugs in the in-house SIEM tool in SISA.

CERTIFICATION

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

Security Information Event Management
RSA NetWitness Suite

EDUCATION

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

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

DECLARATION

I declare the above-furnished information is completely true to my knowledge and I'm confident about it.