OM KANT SHARMA

**SOC Analyst L1**

**Cyber Security, VAPT &**

**Data analyst DS ML AI**

(SIEM Tools- QRadar, Splunk)

Aim towards opportunities that will help me acquire relevant skills and expertise that will help me to utilize my

knowledge, skills and attitude toward the growth of the organization

## Professional Summary

* Worked in 24x7 operational support
* Working on incidents and reviewing the alerts and do detailed analysis on alerts.
* Hands on experience on the Incident Response activities like malware analysis, phishing analysis.
* Good Knowledge on TCP/IP, security concepts, WAN and LAN concepts, Routing protocols
* Firewall security policies.
* Working on assign ticket queue and Understanding and exceeding expectations on all tasked SLA commitments.
* Escalating issues to level 4 and management when necessary.
* Monitor real-time security events on SIEM (Splunk & QRadar) console and Event Analysis and Investigating and mitigation.
* Good understanding on different types of attacks and MITRE, Cyber Kill chain frameworks
* Strong analytical communication and organizational abilities. Knowledge of application, network and endpoint security controls.
* Good knowledge in security solution implementation and handling.

# SKILLS

**SOC Tool: Splunk, Qradar, Proxy, XDR, EDR, Threat Intel, MDR, Firewall, NDR WAPT: Burp suite, SQLmap, Nikto, WPScan, Hydra**

**VAPT: Parrot, Kali Linux Toolkit (Nmap, Wireshark, Slowloris,**

**Metasploit, Nessus)**

**Memory Analysis Tools (Forensic): Volatility, Autopsy, MiniTool**

**Power Data Recovery**

**Network: LAN, WAN switching technologies, IP Routing, IP services**

# CERTIFICATION

* Certfied Ethical Hacker CEH v12 (Provided by ITU) – March 30, 2025

<https://shorturl.at/cgXjw>

* Certified CompTIA Security SY0-701 (Provided by ITU) – March 19, 2025

[**https://shorturl.at/jEKI4**](https://shorturl.at/jEKI4)

* Certified IBM QRadar (CESIENIIN, provided by IBMCE) – August 20, 2023

<https://shorturl.at/98DF0>

* Certified in Ethical Hacking Essentials (EHE), provided by EC-Council – 13th Mar 2024
* <https://shorturl.at/8KH7p>
* Certified in Digital Forensic Essentials (DFE), provided by EC-Council – 15th Mar 2024 <https://shorturl.at/1wEej>

**+91- 8128785346**

[***omkantsharma@gmail.com***](mailto:omkantsharma@gmail.com) ***https://github.com/omkantsharma*** Permanent Addr- Vill- Baroh, P.O- Parwin, Teh-

Barsar, Distt-Hamirpur (Himachal Pradesh) 176040.

Current Addr– Vill- Haweli,P.O- Mahilpur, Distt-

Hoshiarpur, Punjab, 146105.

### PREVIOUS EXPERIENCES

**Aim2Excel, Gurgaon— *Researcher***

Feb to April- 2020

https://shorturl.at/1pfw9

**Tulsi Psychiatric & Rehabilitationcenter -** Mar- 2017 to Dec -2019

https://www.shorturl.at/shortener.php

### EDUCATION

**Uttaranchal University,** Dehradun **—**

Pursuing online MCA (Master of Computer Application) 2024 - 2026

**Gurukul Kangri Vishwavidyalaya,** Haridwar —

*M.A. Psychology* March 2012 - 2014.

**Publication-** https://journal.iaimnumetrolampung.ac.id/index.php/igcj/article/view/1243

Moon Light College, Hamirpur — **Post Graduate Diploma in Computer Application,** March -2011 - 2012

https://drive.google.com/file/d/1fZQGbnza4LF\_w5yRPV1yB-xxujLvLQ3b/view?usp+=drivesdk

**Govt College, Hoshiarpur (Punjab) —**

***Graduation***, March2009 - 20011

**Sen. Sec. School, Bijhari, (Himachal Pradesh) — *Inter matriculation***, March 2008- 2009

* Python, Data Science, Machine Learning, Artificial Intelligence - APTRON, Sec- 15, Noida, (5-2- 2021 - 24- 4-2021)

<https://shorturl.at/mPwI4>

# PROFESSIONAL EXPERIENCE

## Current employment:

**( SOC Analyst –L1 ) & VAPT at All Soft Solutions-IBM Partner**

May 2022 to Present

**Qradar, Splunk, SentinelOne, Crowdstrike, ServiceNow, Jira, ELK, Wazuh, Bluecoat & Zscaler proxy, XOAR, Vectra, Stealth Bit, CISCO Umbrella, Cortex XDR, Wildfire, MS ATP , MITRE, GDPR**

## Duties Performed:

Real-Time Monitoring, Monitor security alerts using SIEM tools like Splunk, QRadar, or Elastic Stack, Identify and analyze potential threats, anomalies, and breaches.

**Incident Triage and Analysis**: Investigate alerts to determine validity and severity, Use threat intelligence and logs to correlate data and identify Indicators of Compromise (IoCs)

**Incident Escalation**:- Escalate confirmed incidents to senior analysts or Incident Response (IR) teams with all relevant details, Work closely with IR teams to contain threats,

**Threat Hunting**: Proactively search for malicious activity within the network, Use frameworks like MITRE ATT&CK for mapping adversarial behavior.

**Report Writing**: Document investigation findings, steps taken, and recommendations, Create weekly and monthly SOC performance reports.

**Log Analysis**: Analyze logs from firewalls, IDS/IPS, endpoints, servers & Nework to identify malicious activities.

**Tool Management**: Manage and maintain SOC tools and dashboards, Fine-tune alert rules to minimize false positives. **Collaboration**: Coordinate with IT, risk management, and compliance teams to enforce security policies, Participate in post-incident reviews to improve processes.

**Vulnerability Management**: Conduct vulnerability scans using tools like Nessus, Qualys, or OpenVAS, Identify, prioritize, and recommend fixes for vulnerabilities.

**Risk Assessment**: Assess potential security risks and recommend mitigations, Perform business impact analysis for critical systems,

**Threat Intelligence**: Research emerging threats and provide updates to the team. Integrate threat feeds with internal security tools.

**Penetration Testing Support:** Assist red teams or external testers with penetration testing efforts, Review test findings and coordinate remediation activities.

**Security Awareness:** Conduct training and awareness programs for employees to reduce human risk factors, Design phishing simulations to test employee responses.

**Forensic Analysis:** Conduct forensic investigations in case of breaches, collect, preserve, and analyze evidence for legal or internal purposes. Tools-volatility, autopsy

### PERSONAL DETAILS

Nationality Indian

Date of Birth: 24/01/1990 Language Known:

**English-***Professional Working Proficiency*

**Hindi-***Full Professional Proficiency*