# CHANDRESH KUMAR KARN

**Cybersecurity Team Lead | SOC Implementation Lead | SIEM Engineering & Threat Detection**

Indore, Madhya Pradesh, India | kumarchandresh227@gmail.com | linkedin.com/in/chandresh-kumar-karn-nmir | github.com/urschandresh

## PROFESSIONAL SUMMARY

Cybersecurity professional with 4+ years of experience across SOC operations, SIEM engineering, and SOC implementation for enterprise US and UK clients at Tata Consultancy Services. Specializes in log source onboarding and integration, threat detection engineering, incident response leadership, use case development, and MITRE ATT&CK-aligned monitoring across IBM QRadar, Splunk, Microsoft Sentinel, Darktrace, and the Palo Alto Cortex suite (XDR/XSIAM/XSOAR). Extends SOC expertise into offensive security through independent Vulnerability Assessment and Penetration Testing (VAPT) engagements. Brings a data-driven edge from a B.Tech in Artificial Intelligence and hands-on Machine Learning/Data Science work, applied to anomaly detection and analytics-driven threat triage. Recognized as "Most Influential Data Analytics Professional" (EIILM Kolkata & CMO Asia) and TCS "Golden Guru" for training and mentorship.

## CORE COMPETENCIES

- SOC Operations & Team Leadership
- Log Source Onboarding & Integration
- Incident Response & Forensic Analysis
- MITRE ATT&CK Tactics & Techniques
- EDR/XDR & Endpoint Security
- Cross-Functional Stakeholder Management
- SIEM Engineering & Administration
- Threat Detection & Use Case Development
- Vulnerability Assessment & Penetration Testing (VAPT)
- Security Risk Assessment & Mitigation
- Security Architecture & Compliance
- Security Awareness Training & Mentorship

## TECHNICAL SKILLS

**SIEM & Security Platforms:** Cortex XSIAM, Sentinel, IBM QRadar (Admin), QRadar on Cloud, Splunk, Microsoft Sentinel, Darktrace EDR, Google SecOps

**Endpoint & XDR:** Palo Alto Cortex XDR, Cortex XSIAM, Cortex XSOAR, EDR/XDR platforms, Microsoft Defender

**Identity, Cloud & Network Security:** Microsoft Entra ID, Active Directory, Microsoft 365 Security, Microsoft Azure, Zscaler, Cisco IronPort, IDS/IPS, DLP, Firewalls

**Frameworks & Methodologies:** MITRE ATT&CK, VAPT Methodology, CVSS Risk Rating, ITIL-aligned Incident Response, Risk Assessment

**Scripting & Automation:** Python, PowerShell, Bash, XQL, AQL, SQL/MySQL

**Tools & Platforms:** ServiceNow, Linux/Unix, Jupyter Notebook, Anaconda, Git/GitHub

## PROFESSIONAL EXPERIENCE

### SOC Implementation Lead – US Client

**Jan 2026 – Present**

*Tata Consultancy Services Ltd. | Indore, India*

- Lead end-to-end onboarding and integration of log sources — servers, network devices, and security tools, to establish comprehensive enterprise security visibility.
- Configure and validate log ingestion across Syslog, API, and agent-based collection methods, ensuring reliable log flow into the SIEM environment.
- Own log parsing, normalization, and event categorization to strengthen correlation rule accuracy and downstream threat detection.
- Troubleshoot log ingestion failures, parsing errors, and EPS fluctuations to sustain continuous, uninterrupted monitoring coverage.
- Partner with infrastructure, network, and application teams to coordinate secure log forwarding and successful security tool integration.
- Perform post-integration validation and testing to confirm event visibility, rule triggering, and monitoring readiness before go-live.
- Maintain integration documentation and configuration standards to support operational continuity and SOC knowledge transfer.

**SOC Engineer – US Client** **Feb 2024 – Dec 2025**

*Tata Consultancy Services Ltd. | Indore, India*

- Directed monitoring and analysis of network traffic, system logs, and security events across enterprise environments, driving early identification of incidents and vulnerabilities.
- Led incident response end-to-end — forensic analysis, root cause identification, and remediation strategy — for security incidents affecting global client environments.
- Oversaw the vulnerability assessment process and delivered Weekly/Monthly security posture reports directly to customers.
- Managed and optimized security technologies including firewalls, IDS/IPS, and DLP systems to keep controls aligned with business and compliance requirements.
- Participated in security architecture design for new systems, ensuring alignment with organizational and compliance standards.
- Designed and delivered security awareness training programs, building a stronger security culture across the organization.
- Coordinated concurrent US and UK client projects using IBM QRadar, Darktrace, and ServiceNow, mentoring junior analysts and reporting performance against SLAs.

**SOC Analyst – US & UK Clients (Offsite)** **Aug 2022 – Feb 2024**

*Tata Consultancy Services Ltd. | Indore, India*

- Monitored and triaged network traffic, system logs, and security events to detect and escalate potential incidents and vulnerabilities across two concurrent client environments (US and UK).
- Investigated and responded to security incidents through forensic analysis, root cause analysis, and remediation, using IBM QRadar, Darktrace, and ServiceNow.
- Conducted vulnerability assessments and delivered Weekly/Monthly findings reports to customers, tracking risk trends over time.
- Implemented and maintained security technologies (firewalls, IDS/IPS, DLP) and contributed to security architecture reviews for new systems and applications.
- Authored and maintained documentation for security policies, procedures, incident response plans, and risk assessments.

**Independent Security Consultant (Freelance) – VAPT** **Jan 2024 – Present**

*Self-Employed | Confidential Client (NDA)*

- Conduct independent Vulnerability Assessment and Penetration Testing (VAPT) engagements outside primary employment, most recently covering 3 network segments and 112 assets for a confidential client.
- Perform network and host-level vulnerability discovery, mapping findings to a structured, CVSS-aligned risk-rating scale (Critical, High, Medium, Low, Informational).
- Identified and reported Critical-severity findings, including a remote code execution exposure, with prioritized, actionable remediation guidance.
- Deliver a full engagement package per assessment: consolidated technical report, remediation guide, and executive briefing tailored for both technical and non-technical stakeholders.
- Apply SOC-honed threat context (MITRE ATT&CK, log-source visibility gaps) to connect offensive findings back to real-world detection and monitoring blind spots.

## CERTIFICATIONS & TRAINING

**Cloud & Security:** Microsoft Azure Certification (TCS/Microsoft), Software Security Assurance (TCS HiTech), Unix/Linux Basics (RedHat)

**Data & AI:** Data Science Specialization – University of Michigan (Coursera), Applied Machine Learning in Python – University of Michigan (Coursera), R Programming – Johns Hopkins University (Coursera), Introduction to Machine Learning – Duke University (Coursera)

**Professional Development:** Business Communication (TCS), Machine First and Intelligent Business Processes (TCS)

## EDUCATION

**B.Tech, Artificial Intelligence** **2018 – 2022**

*Sage University, Indore, Madhya Pradesh, India | 90% Aggregate*

## ACHIEVEMENTS & RECOGNITION

- Most Influential Data Analytics Professional – Asia Pacific (EIILM Kolkata & CMO Asia, Sep 2024): invited guest speaker and panelist for contributions to data analytics.

- Golden Guru 2023 (TCS): recognized for voluntarily training unallocated TCS associates in Python and Machine Learning.
- Xperience Learner (TCS, Nov 2022): completed advanced technical courses, ranked among top performers company-wide.
- Sage Career Day 2025: recognized as Best Student of the 2018–2022 term for academic and cybersecurity performance.
- 1st Rank, Micro Focus International plc Research Paper Writing Competition (2020) for "Classification of Shoppers' Intention."

## NOTABLE TECHNICAL PROJECTS

- AI Virtual Painter (Patented) – Gesture-controlled painting application using computer vision; final-year minor/major project.
- Real-Time Face Mask Detection System – Computer vision model for real-time compliance monitoring.
- Smart Blind Stick & Glasses – Sensor-based IoT assistive device for visually impaired users.
- Bulk IP/URL/Domain Reputation Checker – Python-based tool for batch reputation lookups against threat intelligence sources, streamlining SOC triage of suspicious indicators.
- LogSense – Log analysis utility for parsing and surfacing anomalies in security event data to speed up detection workflows.
- Domain Security Checker – Automated scanner assessing domain security posture (DNS, SSL/TLS, and related configuration checks).
- Threat Intel Platform – Centralized platform for aggregating and correlating threat intelligence feeds to support proactive detection and use case development.