CHANDRESH KUMAR KARN

Cybersecurity Engineer | SOC & Detection Engineering | SIEM/SOAR | Incident Response | Security Automation

Indore, Madhya Pradesh, India | ck.karn@urstrulychandresh.com | linkedin.com/in/chandresh-kumar-karn-nmir | github.com/urschandresh | securewithck.com

PROFESSIONAL SUMMARY

Cybersecurity engineer with 4+ years of experience across SOC operations, SIEM engineering, and detection engineering for enterprise clients at Tata Consultancy Services. Leads end-to-end log source onboarding and SIEM integration, builds and tunes correlation rules and use cases, and drives incident response and threat investigation aligned to the MITRE ATT&CK framework. Works hands-on across IBM QRadar, Microsoft Sentinel, Splunk, Darktrace, and the Palo Alto Cortex suite (XSIAM, XDR, XSOAR), with scripting in Python, PowerShell, and Bash to support security automation. Extends this SOC and detection foundation into offensive security and governance through independent VAPT, GRC, and data privacy advisory engagements, and communicates security posture and findings clearly to both technical and executive stakeholders. Brings an added analytical edge from a B.Tech in Artificial Intelligence and applied machine-learning background, supporting anomaly-informed detection and data-driven threat triage.

CORE AREAS OF EXPERTISE

Security Operations: SOC Operations · Security Monitoring · Incident Triage · Incident Response · Root Cause Analysis · Security Investigation · Threat Hunting · Security Operations Leadership

Detection Engineering: Threat Detection · Detection Engineering · Use Case Development · Correlation Rules · Detection Tuning · MITRE ATT&CK · Alert Investigation

SIEM / XDR / SOAR: Cortex XSIAM · Cortex XDR · Cortex XSOAR · IBM QRadar · QRadar on Cloud · Microsoft Sentinel · Splunk · Google SecOps · Darktrace

Log Management & Integration: Log Source Onboarding · Log Source Integration · Syslog · API Integration · Agent-Based Collection · Log Parsing · Normalization · Event Categorization

Endpoint, Identity & Network Security: Microsoft Defender · Microsoft Entra ID · Active Directory · Microsoft 365 Security · Zscaler · Cisco IronPort · IDS/IPS · DLP · Firewalls

Security Engineering & Automation: XQL · AQL · Python · PowerShell · Bash · SQL · Security Automation

Governance, Risk, Compliance & Data Privacy: GRC Advisory · ISO 27001 · SOC 2 · NIST CSF · PCI-DSS · GDPR · India's DPDP Act · Controls & Policy Assessment · Risk Assessment

Frameworks & Methodologies: MITRE ATT&CK · CVSS · Vulnerability Assessment · VAPT · Risk Assessment · Security Architecture

TECHNICAL SKILLS

SIEM: IBM QRadar (Admin), QRadar on Cloud (QRoC), Microsoft Sentinel, Splunk, Google SecOps

XDR / EDR / SOAR: Palo Alto Cortex XSIAM, Cortex XDR, Cortex XSOAR, Darktrace EDR, Microsoft Defender

Detection & Query Languages: XQL, AQL, SQL/MySQL, MITRE ATT&CK-aligned Use Case Development

Identity & Endpoint Security: Microsoft Entra ID, Active Directory, Microsoft 365 Security, Microsoft Azure

Network & Email Security: Zscaler, Cisco IronPort, IDS/IPS, DLP, Firewalls

Scripting & Automation: Python, PowerShell, Bash

GRC & Data Privacy: ISO 27001, SOC 2, NIST CSF, PCI-DSS, GDPR, India's DPDP Act

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

Operating Systems / Platforms: Linux/Unix, Jupyter Notebook, Anaconda, Git/GitHub

ITSM / Workflow: ServiceNow

PROFESSIONAL EXPERIENCE

SOC Implementation Lead — Multiple Clients

Jan 2026 – Present

Tata Consultancy Services Ltd. | Indore, India

- Lead end-to-end log source onboarding and SIEM integration across servers, network devices, and security tools, establishing enterprise-wide security visibility for a global SOC implementation program.
- Engineer and validate log ingestion pipelines across Syslog, API, and agent-based collection methods, troubleshooting ingestion and parsing issues to maintain reliable SIEM visibility and detection coverage.
- Own log parsing, normalization, and event categorization to strengthen correlation rule accuracy and downstream threat detection engineering.
- Troubleshoot log ingestion failures, parsing errors, and EPS fluctuations to sustain continuous, uninterrupted monitoring coverage across onboarded log sources.

- Coordinate with infrastructure, network, and application teams to plan secure log forwarding and drive successful security tool integration.
- Conduct post-integration validation and testing — confirming event visibility, correlation rule triggering, and monitoring readiness — before production go-live.
- Maintain integration documentation and configuration standards, supporting operational continuity and SOC knowledge transfer.

SOC Engineer — US & SG Clients **Feb 2024 – Dec 2025**

Tata Consultancy Services Ltd. | Indore, India

- Directed enterprise-wide monitoring and analysis of network traffic, system logs, and security events, enabling early identification and triage of incidents and vulnerabilities.
- Led incident response end-to-end — forensic analysis, root cause identification, and remediation strategy — for security incidents across global client environments.
- Owned the vulnerability assessment lifecycle and delivered Weekly/Monthly security posture reports directly to customer stakeholders.
- Managed and tuned security technologies including firewalls, IDS/IPS, and DLP systems to keep controls aligned with business and compliance requirements.
- Contributed to security architecture design for new systems, ensuring alignment with organizational and compliance standards.
- Designed and delivered security awareness training programs, strengthening organizational security culture.
- Coordinated concurrent US and SG client SOC operations 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 incidents and vulnerabilities across two concurrent client environments (US and UK).
- Investigated and responded to security incidents using IBM QRadar, Darktrace, and ServiceNow, applying forensic analysis and root cause analysis to drive remediation.
- 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, GRC & Data Privacy **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).
- Identify and report 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 technical and non-technical stakeholders.
- Apply SOC-honed threat context (MITRE ATT&CK, log-source visibility gaps) to connect offensive findings to real-world detection and monitoring blind spots.
- Completed a separate, environment-wide Governance, Risk & Compliance (GRC) and data privacy advisory engagement (NDA), assessing and aligning client security controls and data-handling practices against ISO 27001, SOC 2, NIST CSF, and PCI-DSS, alongside GDPR and India's DPDP Act data privacy requirements.

SELECTED SECURITY ENGINEERING PROJECTS

Secure-One — *Local-First Endpoint Security / XDR Platform (Independent Project)*

- Building a Windows-focused, local-first endpoint security/XDR platform incorporating security telemetry, detection engineering, and behavioral NGAV concepts.
- Implements threat intelligence correlation, active response, and quarantine, alongside host firewall controls, domain/IP blocking, and host isolation within SOC-oriented security workflows.

Bulk IP/URL/Domain Reputation Checker — *Python*

- Python-based threat intelligence and reputation utility for batch lookups against threat intelligence sources, streamlining SOC triage of suspicious indicators.

LogSense — *Security Log Analysis Utility*

- Log analysis utility that parses security event data and surfaces anomalies, speeding up investigation and detection workflows.

Domain Security Checker — *Automated Security Posture Scanner*

- Automated scanner assessing domain security posture, including DNS, SSL/TLS, and related configuration checks.

Threat Intelligence Platform — *Aggregation & Correlation*

- Centralized platform concept for aggregating and correlating threat intelligence feeds to support proactive detection and use case development.

CERTIFICATIONS & CREDENTIALS

- Microsoft Azure Certification (TCS / Microsoft)

SELECTED PROFESSIONAL TRAINING

- Software Security Assurance — TCS HiTech
- Unix/Linux Basics — RedHat
- 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)
- 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."

ADDITIONAL 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.