RAHUL KUMAR RAM

+91 99999 99999 | Email | LinkedIn | Github | Portfolio | Bihar, India

SUMMARY

Entry-Level SOC Analyst with hands-on experience in SIEM monitoring, alert triage, incident investigation, and threat detection using Microsoft Sentinel, Splunk, QRadar, and Snort. Skilled in log analysis, incident response, vulnerability management, and security operations, with a strong understanding of the MITRE ATT&CK and Cyber Kill Chain frameworks.

EDUCATION

All Saints' College of Technology Bhopal, MP
B.Tech, Computer Science & Engineering *2021 – 2025*

EXPERIENCE

Cyber Security Analyst (Intern) Aug 2024 – Sep 2025
NIELIT - Kolkata *West Bengal*

- Continuously monitored **Microsoft Sentinel**, Snort IDS/IPS, and log sources for suspicious activity; performed initial alert triage and severity classification, escalating validated incidents with SOC playbooks and escalation matrix
- Verified log ingestion and forwarding from SIEM, IDS/IPS, and EDR platforms; identified tool and data gaps, contributing to prevention of **150+ security incidents**
- Maintained SOC case records and escalation workflows, identified false-positive patterns, and delivered **100+ cybersecurity training sessions,** for the **Indian Army Officers**

SOC Trainer - Cyber Security & Ethical Hacking Jan 2026 – May 2026
NIELIT | I4C-Sponsored National Cybercrime Investigation Program *Bihar*

- Served as first point of contact for security incident analysis for **130+ state police personnel** (Constables, SI, CID, STF), delivered SOC-aligned training covering threat detection, OSINT, network forensics
- Developed and updated SOC runbooks, incident playbooks, and daily/weekly security reports and dashboards; improved case-handling efficiency by ∼**65%** and reduced investigation turnaround by ∼**40%** - maintaining **90%+ SLA completion** across 5 batches

PROJECTS

Microsoft Sentinel SIEM | Github Repo - Azure Sentinel 2026 - Present

- Provisioned a full Azure Sentinel environment - Resource Group, Log Analytics Workspace, Sentinel Workspace, and Azure RBAC roles; integrated Content Hub data connectors and ingested Microsoft Entra ID (Azure AD) logs with DCR configuration
- Ingested live threat intelligence feeds, validated TI log ingestion, and developed KQL-based detection rules to surface high-priority alerts; documented all configurations, connector setups, and findings in detailed lab walkthroughs

Custom SIEM Platform | Github Repo - Splunk, Log Correlation, Automated Alert Escalation 2025

- Architected a Splunk-based SIEM for real-time log ingestion, event correlation, and automated alert escalation; implemented detection rules with ticketing integration and SOC dashboard metrics, mirroring enterprise L1 SOC triage and reporting workflows

Network Intrusion Detection System (NIDS) | Github Repo - Snort, IDS/IPS, Rule Engineering 2024

- Configured a production-grade Snort NIDS with custom detection rules for continuous network monitoring; automated alarm generation and reduced false-positive noise through documented suppression rules

TECHNICAL SKILLS

SIEM & SOC: Microsoft Sentinel, Splunk, QRadar, Snort IDS/IPS, EDR, Firewall Monitoring, Alert Triage, Incident Escalation, L1 SOC Operations, Threat Detection, CrowdStrike, Microsoft Defender, Active Directory

Incident Management: SOC Case Management, Playbook Development, Escalation Matrix, False Positive Management, Phishing & URL Analysis

Cloud & Identity: Azure Log Analytics Workspace, Azure RBAC, Entra ID (Azure AD), Data Connectors, DCRs, Content Hub, Threat Intelligence, IAM, MFA, Role-Based Access Control

Scripting & Automation: Python, PowerShell, Bash, KQL, Security Workflow Automation, Custom Connector Development

Vulnerability Management: Vulnerability Scanning, Severity Assessment, Remediation Tracking, Patch Management

Frameworks: MITRE ATT&CK, Cyber Kill Chain, OWASP Top 10, NIST, ISO 27001

CERTIFICATIONS

Microsoft Sentinel - Udemy | 10hrs hands-on lab training | Verify

Ethical Hacking Essentials (EHE) - EC-Council CodeRed | Verify

Network Defense Essentials (NDE) - EC-Council CodeRed | Verify

Google Cyber Security Professional Certificate - Coursera | Verify

Secure Access with Azure Active Directory - Coursera | Verify