Rishabh Yadav

SOC Analyst — Cybersecurity Analyst — Security Operations
Gurugram, Haryana, India
+91-8287564548 — rishabhyadav621@gmail.com
linkedin.com/in/rishabh-yadav-oct — my-writeup.pages.dev

Professional Summary

SOC Analyst with 12+ months cybersecurity experience across JPMorgan Chase, Deloitte, Mastercard, and Infosys programs. Experience in SIEM monitoring, security alert triage, incident response, and threat detection across multiple log sources including Windows Event Logs, firewall logs, DNS logs, and authentication records. Investigated phishing campaigns, malware indicators, and unauthorized access attempts using Splunk, ELK Stack, and Wireshark. CEH certified cybersecurity graduate skilled in MITRE ATT&CK mapping, vulnerability management, and network traffic analysis. Seeking SOC Analyst L1 or Cybersecurity Analyst role in enterprise security operations.

Core Competencies

- Security Operations Center (SOC) Monitoring
- SIEM Monitoring and Alert Triage
- Incident Response Lifecycle (NIST Framework)
- Threat Detection and Threat Hunting
- Log Analysis and Event Correlation
- Malware Analysis Fundamentals
- Phishing Detection and Email Security
- MITRE ATT&CK Mapping
- Network Traffic Analysis
- Vulnerability Management

Technical Skills

SIEM and Monitoring: Splunk Enterprise, ELK Stack, Security Event Monitoring, Log Aggregation, Correlation Rules

Security Tools: Wireshark, Nessus, Burp Suite, Metasploit, OWASP ZAP, Snort IDS

Incident Response and Threat Intelligence: MITRE ATT&CK, VirusTotal, MISP, Malware Sandbox Analysis

Operating Systems: Linux, Windows Server, Active Directory, macOS Security Basics

Programming and Scripting: Python, Bash, PowerShell, SQL Basics, Git

Networking: TCP/IP, DNS, HTTP, HTTPS, VPN, Firewall Logs, Packet Analysis

Professional Experience

Cybersecurity Analyst Intern
JPMorgan Chase & Co. May 2023 – July 2023

- Monitored and triaged 150+ SIEM alerts involving phishing attempts, malware indicators, and suspicious login activity across enterprise security dashboards
- Performed log correlation across Windows Event Logs, DNS logs, firewall logs, and proxy logs using Splunk queries
- Investigated 12 phishing campaigns through email header analysis and malicious URL inspection using VirusTotal intelligence
- Reduced mean time to detect security incidents from 45 minutes to 28 minutes through improved alert triage procedures
- Documented 20+ incident investigation cases using ticketing workflows aligned with NIST incident response lifecycle

Cybersecurity and Digital Forensics Intern
Deloitte June 2022 – August 2022

- Analyzed 50+ simulated security incidents including SQL injection, cross site scripting, and insider threat scenarios
- Performed log analysis on large scale Linux and Windows system logs using ELK Stack queries
- Identified 15 privilege escalation attempts and lateral movement indicators through forensic investigation
- Mapped attack techniques to MITRE ATT&CK framework to assist detection rule development
- Documented forensic findings and remediation recommendations for web application vulnerabilities

Cybersecurity Project Intern
Mastercard April 2022 – June 2022

- Conducted phishing detection exercises analyzing 500+ simulated phishing emails to identify high risk user groups
- Reduced phishing click rate by 40 percent through security awareness analysis and mitigation recommendations
- Performed network packet inspection using Wireshark on 5GB PCAP datasets to detect abnormal payment API traffic
- Assisted threat modeling activities on financial transaction systems aligned with PCI DSS security controls

Power Programmer Intern
Infosys May 2022 – June 2022

- Developed 15+ Python automation scripts for log parsing, vulnerability reporting, and automated SOC ticket creation
- Automated threat intelligence enrichment workflows integrating VirusTotal and AbuseIPDB feeds
- Reduced manual security analysis workload by 60 percent across automation workflows

Projects

Poor Man's Pentest Automated VAPT Toolkit

- Built automated penetration testing toolkit using Python and Bash with 25 modules for reconnaissance, scanning, and exploitation
- Integrated Nessus API and Metasploit modules to identify 120+ vulnerabilities across test environments
- Reduced manual penetration testing effort from 4 hours to 30 minutes per target

Pawncat Network Analysis Tool

- Developed Python based network analysis tool using Scapy and socket programming
- Processed more than 100000 packets with real time filtering and protocol inspection
- Simulated command and control traffic to test EDR detection mechanisms

Cybersecurity CTF Lab Environment

- Built home SOC lab with 5 virtual machines generating security logs for SIEM analysis
- Deployed Splunk server and created correlation searches mapped to MITRE ATT&CK techniques
- Investigated malware samples and documented indicators of compromise from CTF challenges

Education

Bachelor of Technology in Computer Science and Engineering
Gurukul Kangri Vishwavidyalaya, Haridwar 2021 – 2025
CGPA: 7.8/10
Relevant Coursework: Network Security, Cryptography, Operating Systems, Computer Networks, Database Systems

Certifications

- Certified Ethical Hacker (CEH) – EC Council
- Certified in Cybersecurity (CC) – ISC2
- Cybersecurity Virtual Experience – JPMorgan Chase
- Cybersecurity Virtual Experience – Mastercard
- STEM Connect Cybersecurity Program – Deloitte
- OWASP Top 10 Security Training – LinkedIn Learning

Leadership

Co Founder and Technical Lead
COMMUNICODE GKV Cybersecurity Club

- Built cybersecurity community growing from 0 to 400+ members
- Organized 24 technical workshops on SOC operations, penetration testing, and malware analysis
- Coordinated 8 capture the flag competitions involving 200+ participants

Additional Information

Languages: English, Hindi
Availability: Immediate joining and 24/7 rotational SOC shifts
Location Flexibility: Open to relocation across India or remote SOC roles