HARDEE N. HATODE

Mumbai, India
+91 8451866209 | hardeehatode1611@gmail.com
hardee.co.uk | linkedin.com/in/hardee-hatode-315782280

PROFILE

Cybersecurity MSc graduate (Distinction, University of Surrey, NCSC-certified) with practical experience supporting security monitoring, incident detection and vulnerability assessment. Strong technical grounding across SIEM, network analysis and threat identification, with hands-on experience building SOC simulations and analysing real-world attack patterns. Able to communicate technical findings clearly and work effectively in team environments. Seeking an entry-level Security Analyst or SOC Analyst role.

EDUCATION

MSc Cybersecurity (NCSC-certified)
University of Surrey | 2025–2026
Distinction

BSc Computer Science
University of Mumbai | 2021–2024
CGPA: 6.99 / 10

PROFESSIONAL EXPERIENCE

SOC Intern | Talakunchi Networks
Jul 2026 - Present

- Monitored and analysed Imperva WAF events, investigating source IPs, hit counts, attack patterns, ISP information, and threat intelligence to identify suspicious or malicious activity.
- Performed ELK alert monitoring and triage, analysing security events, identifying potential false positives, and documenting findings and required actions.
- Analysed Attack Analytics incidents based on attack type, severity, and incident status, investigating associated IPs and documenting analysis findings during alert acknowledgement.
- Investigated web-based attacks including SQL Injection, correlating WAF activity with VirusTotal reputation, whitelist status, and other indicators to support blocking or monitoring decisions.

RELEVANT EXPERIENCE & PROJECTS

Mini SOC Lab (Splunk SIEM) | 2026

- Built a simulated SOC environment using Splunk, ingesting over 1,500 security events
- Developed detection rules for brute-force attacks, reconnaissance activity and suspicious PowerShell execution
- Created structured incident reports aligned to MITRE ATT&CK to support triage and escalation
- Built and debugged a SOAR automation layer integrating Splunk alerts with IP reputation enrichment and severity-based triage logic, correctly distinguishing escalation-worthy incidents from low-risk false positives

Linux to Windows Log Forwarding Lab (rsyslog / Kiwi Syslog Server) | 2026

github.com/Hardeeh03/soc-lab-log-forwarding

- Built a log forwarding pipeline where an Ubuntu Server VM forwards system and auth logs to a Windows-based syslog collector (Kiwi Syslog Server NG) over UDP port 514 using rsyslog, simulating brute-force SSH login attempts and privilege escalation activity
- Confirmed real-time log ingestion with source IP, severity and facility metadata visible on the collector side, and mapped findings to MITRE ATT&CK T1110
- Demonstrates end-to-end understanding of log collection pipelines used in MSSP/SOC environments prior to SIEM ingestion

IoT Security Research (MSc Dissertation) | 2025

- Designed a smart home test environment using ESP32 devices and MQTT messaging
- Simulated attacks including replay, traffic interception and denial-of-service
- Applied controls such as TLS encryption and access restrictions to mitigate risks
- Produced clear technical analysis of vulnerabilities and recommended secure configurations

Web Security Scanner (Python / OWASP ZAP) | 2024–2025

- Built a web application to identify common vulnerabilities including SQL injection and XSS
- Automated scanning using OWASP ZAP and consolidated results into a central dashboard
- Produced structured reports with prioritised risks and remediation guidance

Network Traffic Analysis (Wireshark) | 2024

- Analysed network traffic across key protocols including DNS, TCP and HTTP/S
- Identified indicators of compromise such as ARP spoofing and unsecured credentials
- Developed practical filtering techniques for detecting suspicious behaviour

ADDITIONAL EXPERIENCE

Student Ambassador – Unilife
Apr 2025 – May 2

- Act as a primary contact for over 100 residents, handling queries and resolving issues
- Supported onboarding activities and coordinated events
- Built strong communication, organisation and stakeholder management skills

TECHNICAL SKILLS

Security & Monitoring: Splunk, SIEM alerting, incident analysis, MITRE ATT&CK, ISO 27001 fundamentals
Security Tools: Wireshark, Nmap, Burp Suite, OWASP ZAP, Metasploit, Kali Linux
Networking: TCP/IP, DNS, HTTP/S, MQTT, packet analysis
Programming: Python, SQL, Kotlin, Java, C, HTML, CSS
Frameworks & Systems: Flask, Django, Node.js, MongoDB, SQLite
Operating Systems: Windows, Linux (Ubuntu, Kali)

CERTIFICATIONS

- Google Cybersecurity Professional Certificate
- Cyber Security Training – Acmegrade

LANGUAGES

English (fluent) | Hindi (native) | Marathi (native)