RASHEED FARHAT

Incident Response Analyst — Endpoint Protection

530-370-5109 | rasheedfrht@gmail.com | linkedin.com/in/rasheed-farhat010 | github.com/RasheedFarhat | medium.com/@rasheed-farhat

Cybersecurity analyst built through CrowdStrike's own Cybersecurity Mentorship Program, practicing incident detection, containment, and escalation on Falcon EDR, Splunk, and Wireshark across simulated Windows/Linux environments. CompTIA Security+ and CySA+ certified, with independent forensic malware analysis, detection-engineering, and agentic-AI (MCP) abuse-detection projects built using AI-assisted workflows. Top-percentile national incident-handling competitor.

CERTIFICATIONS

CompTIA Security+ (2025–2028) • CompTIA CySA+ (2026–2029) • CCNA: Switching, Routing & Wireless Essentials • Linux Professional Certification (Butte College) • Cisco IT Essentials

Pursuing AWS Certified Cloud Practitioner

CORE COMPETENCIES

- **Incident Handling:** End-to-end detection, containment, and escalation across simulated Windows/Linux environments (Falcon EDR, Splunk, Wireshark) and timed national incident-response competitions.
- **Malware & Computer Forensic Analysis:** Static/dynamic APK reverse engineering (ADB, APKTool, JADX, VirusTotal) with IOC extraction and OSINT-based C2 attribution.
- **Network Forensic Analysis:** Deep packet inspection and log correlation (Wireshark, Splunk); de-obfuscated proxy/tunnel telemetry to isolate true attacker IPs for automated enrichment.
- **Incident Remediation & Countermeasures:** Authored and validated Sigma/Wazuh detection rules and IAM deception controls, measured for recall and false-positive rate against labeled data rather than assumed coverage.
- **Systems, Network Architecture & Programming:** Linux/Windows administration, CCNA-level TCP/IP networking and secure architecture, and Python/Bash/PowerShell/Golang/C++ scripting for security automation.
- **AI-Enabled Security Engineering:** Apply agentic AI / AI-assisted workflows (Claude Code) to accelerate detection authoring and validation; hands-on experience detecting abuse of AI-agent (MCP) infrastructure.
- **Technical Communication:** Author detection-engineering write-ups on Medium & LinkedIn (900+ organic impressions/post); two years translating technical issues for a broad, non-technical audience.

KEY PROJECTS

- **Mobile Malware & Forensic Analysis** — *Independent*
  Reverse-engineered a malicious APK from a real infected Android device (ADB, Kali Linux, APKTool, JADX, VirusTotal); extracted IOCs and attributed C2 infrastructure via OSINT, documenting the full static/dynamic analysis chain.
- **MCP-DETECT: Agentic AI (MCP) Abuse Detection** — *github.com/RasheedFarhat, 2026*
  Built a proxy capturing Model Context Protocol tool-calling telemetry and authored 10 Wazuh rules across 5 abuse techniques mapped to the OWASP MCP Top 10; measured 100% recall / 0 false positives on 4,727 records and red-teamed across 12 adversarial evasion classes.
- **Detection-as-Code Pipeline: Sigma → Wazuh** — *github.com/RasheedFarhat, 2025*
  Engineered a Python compiler and CI/CD pipeline translating 58 Sigma rules into 216 production Wazuh rules across 119 MITRE ATT&CK techniques, backed by 87 automated tests and a dry-run-first deployment process.

EXPERIENCE

Cybersecurity Mentorship Program — CrowdStrike (Remote) **Oct 2024 – Apr 2025**

- Practiced incident detection, containment, and escalation workflows using Falcon EDR, Splunk, and Wireshark across simulated Windows/Linux enterprise environments; correlated alerts to map adversarial lateral movement.
- Participated in red team/blue team tabletop simulations and built career/skill-development plans directly alongside CrowdStrike mentors, gaining first-hand familiarity with the Falcon platform and virtual SOC cadence.

National Cyber League (NCL) — Competitor **Spring & Fall 2024**

- Triaged timed, scenario-based network traffic analysis, log/alert review, cryptography, and OSINT challenges; ranked in the top percentile nationally among thousands of competitors.

Front Desk & Communications Support — STEM Dept., Butte College **Oct 2023 – Feb 2025**

- First point of contact for a high-volume flow of student, faculty, and staff inquiries; independently triaged, prioritized, and routed requests with clear written/verbal communication, without direct supervision.

TECHNICAL SKILLS

Detection & SIEM: Wazuh, Splunk, Sigma, Wireshark

Forensics & Malware: ADB, APKTool, JADX, VirusTotal, Kali Linux

Programming & Systems: Python, Bash, PowerShell, Golang, C++ | Linux, Windows, TCP/IP, Cisco IOS

Identity, Cloud & Frameworks: Authentik (IAM/SSO), AbuseIPDB API, AWS (in progress), MITRE ATT&CK, OWASP MCP Top 10

EDUCATION

Associate of Science, Cybersecurity and Information Assurance — Butte College, Oroville, CA **Aug 2021 – Dec 2024**

Concurrent coursework, California State University, Chico • Dean's List, 4.0 GPA (Spring 2024) • NCL Games Scholarship, ISACA Foundation (2024)