Bhadreshkumar Ghevariya

(226) 808-5897 | bhadreshkumarghevariya@gmail.com
linkedin.com/in/bhadreshghevariya | github.com/bhadreshkumarghevariya

SUMMARY

SOC-focused security practitioner with CompTIA Security+ and hands-on detection experience from a self-built Wazuh SIEM lab and a completed information security analyst program. Skilled in log analysis, alert triage, threat detection, incident response, and mapping adversary behavior to the MITRE ATT&CK framework. Full-stack development background brings a builder's understanding of how systems are architected and how they are attacked. Seeking a SOC Analyst role to contribute from day one.

TECHNICAL SKILLS

Security & SOC: Wazuh SIEM, MITRE ATT&CK, log analysis, alert triage, threat detection, incident response & escalation, brute-force detection, packet analysis (Wireshark)

Systems & Networking: Linux (Ubuntu Server), Windows, macOS, TCP/IP, DNS, DHCP, SSH, hardware troubleshooting, mesh VPN (Tailscale / WireGuard)

Tools & Development: Git, Linux CLI, JavaScript, ReactJS, NodeJS, MongoDB, REST APIs, Agile

CERTIFICATIONS & TRAINING

CompTIA Security+ (SY0-701)

Information Security Analyst Program — Correlation One (sponsored by Amazon Career Choice)

- Completed a rigorous SOC-focused program covering threat detection, log analysis, incident response, SIEM operations, and MITRE ATT&CK, mapped to SOC Tier 1 responsibilities.

SECURITY PROJECTS & HOME LAB

Home SOC Lab — Wazuh SIEM | *Wazuh, Ubuntu Server, Linux, MITRE ATT&CK*

- Deployed a single-node Wazuh SIEM (indexer, manager, dashboard) on a self-provisioned Ubuntu Server host, configured for headless remote administration.
- Simulated SSH brute-force attacks and validated the full detection pipeline: log collection, rule matching, alert correlation, and triage.
- Distinguished single authentication failures (rule level 5) from correlated brute-force activity (rule level 10), mapped to MITRE ATT&CK T1110 (Credential Access).
- Triaged raw alerts to extract source IP, targeted account, and technique, reflecting core SOC Tier 1 workflows.
- Configured secure remote access using a WireGuard-based mesh VPN (Tailscale), with no ports exposed to the public internet.

ProSystemz — Custom PC Builder Platform | *ReactJS, NodeJS, MongoDB, GraphQL, Stripe*

- Built a full-stack e-commerce platform implementing authentication, API security, and role-based access control across user and vendor roles.
- Integrated payment processing and debugged cross-system data flows; secured checkout with Stripe.
- Created a vendor dashboard for real-time inventory management across 50+ product listings.

PROFESSIONAL EXPERIENCE

Amazon | FC Associate Oct 2024 – Present

Toronto, ON, Canada

- Diagnosed and escalated technology malfunctions following structured escalation procedures, supporting rapid resolution for operations teams.
- Maintained data accuracy across integrated warehouse management systems while processing thousands of items per shift under time pressure.
- Trained and assisted 10+ peers on device troubleshooting procedures, improving team self-sufficiency.

EDUCATION

Conestoga College, Ontario, Canada | Web Development Diploma May 2022 – Aug 2023

Uka Tarsadia University, India | B.Sc. Information Technology Jul 2018 – Jun 2021