Jordan Blake

Entry-Level Security Operations Center (SOC) Analyst

jordan.blake@email.com • (555) 987-6543 • linkedin.com/in/jordan-blake • Remote / Willing to relocate

Professional Summary

Motivated and analytical SOC Analyst with hands-on experience monitoring security telemetry, triaging alerts, and supporting incident response processes at a corporate Security Operations Center. Familiar with Splunk, EDR platforms, and MITRE ATT&CK; mapping. Strong foundation in network fundamentals, scripting (Python/Bash), and security best practices. Quick learner eager to contribute to detection tuning and threat-hunting initiatives.

Professional Experience

Security Operations Center (SOC) Analyst — E Corp (Corporate) June 2025 — Present

- Monitor SIEM dashboards and security alerts (Splunk) across enterprise telemetry; triage and classify alerts using established playbooks.
- Perform initial incident validation and escalation; create and update tickets with evidence, impact, and remediation steps in the ticketing system.
- Conduct basic host and network level investigations using EDR, Wireshark, and log analysis; preserve artifacts for senior analysts when needed.
- Tune correlation rules and suppress false positives; document changes and measure impact on alert volume and signal-to-noise ratio.
- Map observed behaviors to MITRE ATT&CK; to support consistent incident categorization and reporting.

IT Security Intern — MidMarket Tech (Internship) Jan 2024 — May 2025

- Assisted with phishing simulation program and analyzed results to recommend targeted training.
- Developed Python scripts to aggregate and normalize log exports for easier review in Splunk.
- Supported patch verification and baseline hardening checks on Windows and Linux systems.

Education

B.S. in Cybersecurity State University — 2024

Relevant coursework: Network Security, Digital Forensics, Operating Systems, Incident Response.

Certifications

- CompTIA Security+ (SY0-601) — 2025
- Splunk Fundamentals 1 — 2024
- AWS Certified Cloud Practitioner — 2024 (basic cloud security familiarity)

Technical Skills

- Security tools: Splunk SIEM, ELK (basic), CrowdStrike Falcon (EDR), Wireshark, Suricata/Zeek
- Languages & scripting: Python, Bash, basic PowerShell
- Concepts: Incident Triage, Threat Hunting, MITRE ATT&CK;, Log Analysis, IDS/IPS, Network fundamentals (TCP/IP)
- Platforms: Windows, Linux (Ubuntu/CentOS), basic AWS familiarity
- Soft skills: Clear written reporting, cross-team escalation, rapid learning, documentation

Selected Projects & Labs

- SIEM Rule Tuning — Built and tuned correlation searches in Splunk to reduce phishing-related false positives by ~30% in lab environment.
- Malware Analysis Lab — Performed static and dynamic analysis exercises on benign samples; documented IOC extraction and containment steps.

• Automated Log Normalizer — Python script to ingest CSV log exports, standardize fields, and push into test Splunk index.

Additional

• Availability: Full-time, flexible hours (experienced with rotating shifts).
• References available upon request.

Resume generated: October 05, 2025