Jordan Abernathy-Cruz

SOC Analyst I | IT Support Technician

jordan.abernathycruz@email.example • (512) 555-0117

PROFESSIONAL SUMMARY

Tier 1 SOC analyst with one year of alert triage after two years in IT support. Investigates phishing, endpoint and identity alerts in Splunk and CrowdStrike, writes clear tickets for escalation and automates small tasks with Python. Security+ and CySA+ certified, and builds detection skills in a home lab.

EXPERIENCE & PROJECTS

Lonestar Managed Security · Austin, TX **Sep 2025 — Present**

SOC Analyst I

- Triage 40 to 70 SIEM and EDR alerts per shift for 15 client environments, closing false positives with documented evidence and escalating real threats to tier 2.
- Investigated a credential phishing campaign hitting three clients, pulling indicators from headers and URLs and blocking them before any account was used.
- Wrote a Python script that enriches alert tickets with IP and domain reputation, saving several minutes per investigation for the whole shift.
- Mapped recurring alert types to MITRE ATT&CK techniques and suggested two Splunk rule tunings that the detection team adopted.

Colorado River Medical Group · Round Rock, TX **Jun 2023 — Aug 2025**

IT Support Technician

- Resolved desktop, account and network tickets for 300 clinic staff, including password resets and multifactor enrollment under HIPAA access rules.
- Reported suspicious emails and unusual logins to the security team, and helped run phishing awareness sessions for front-desk staff.

Detection home lab

- Built a lab with a Windows domain, Sysmon and an open-source SIEM to simulate attacks with Atomic Red Team and write detections for them.

EDUCATION

BS, Cybersecurity **2023**

Central Texas State University

SKILLS

Technical: Splunk, CrowdStrike Falcon, Microsoft Defender, Phishing analysis, Alert triage, MITRE ATT&CK, Wireshark, Active Directory, Python, PowerShell, Linux, Ticketing (ServiceNow)

Certifications: CompTIA Security+ · CompTIA CySA+