Darnell Hughes

darnell.hughes@email.com · (210) 555-0137 · San Antonio, TX · linkedin.com/in/darnellhughes

September 15, 2026

USAA
San Antonio, TX

Re: Cybersecurity Analyst, Security Operations Center

Dear Hiring Manager,

Your posting for a Cybersecurity Analyst on the SOC team asks for someone who can take an alert from Splunk and CrowdStrike and carry it through to containment. That is the work I have done for the past three years at Brazos Health System, where I am a Security Analyst II covering 9 hospitals and about 14,000 endpoints.

Most of our serious incidents start with a phishing email, as I expect many of yours do. Last year a vendor's compromised mailbox sent invoice lures to our finance staff. I traced the sign-ins in Entra ID, disabled three accounts that had entered credentials, purged 1,140 copies of the message and wrote the incident summary our privacy office used for its HIPAA review. Afterward I built a Splunk SOAR playbook for user-reported phish, which brought our median time to a verdict from 40 minutes to 9.

Before Brazos I spent almost three years at a managed security provider watching Sentinel and QRadar for 30 clients. The volume taught me to separate noise from signal quickly; the Cobalt Strike beacon I found in one client's DNS logs taught me to keep looking when something feels slightly off. I have since written 22 correlation searches mapped to MITRE ATT&CK and retired the rules that were wasting analysts' time.

I hold Security+, CySA+ and GCIH, and I would like to bring this experience to a team protecting members' money and accounts. I am in San Antonio and can meet whenever it suits your schedule.

Sincerely,

Darnell Hughes