Darnell Hughes

Security Analyst II · SOC Operations & Incident Response

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

SUMMARY

Security analyst with 6 years in security operations, the last 3 on a hospital system's internal SOC. Works in Splunk Enterprise Security, CrowdStrike Falcon and Microsoft Sentinel daily. Strongest in detection tuning and containing phishing and account compromise incidents.

EXPERIENCE

Security Analyst II · Brazos Health System — Mar 2023 – Present
San Antonio, TX

- Triaged about 60 escalated alerts a week from Splunk ES and CrowdStrike Falcon across 9 hospitals and 14,000 endpoints.
- Contained a 2025 business email compromise: disabled 3 Entra ID accounts, purged 1,140 phishing messages and drafted the HIPAA incident summary.
- Wrote 22 Splunk correlation searches mapped to MITRE ATT&CK and retired 9 noisy rules, dropping weekly false positives from about 480 to 190.
- Ran monthly Tenable scans and chased remediation with server teams; critical findings older than 30 days fell from 87 to 12 in a year.
- Automated phishing-report handling with a Splunk SOAR playbook, bringing median time to verdict from 40 minutes to 9.

SOC Analyst I · Pinnacle Managed Security — Jun 2020 – Feb 2023
San Antonio, TX

- Monitored Microsoft Sentinel and QRadar queues for 30 client tenants on a rotating 12-hour shift schedule.
- Closed an average of 35 tier 1 alerts per shift, escalating confirmed intrusions with PCAPs and timeline notes attached.
- Caught a Cobalt Strike beacon at a manufacturing client from DNS beaconing in proxy logs; 4 hosts were isolated within 2 hours.

Help Desk Technician · Mission Creek ISD — Jun 2018 – May 2020
San Antonio, TX

- Handled 25 to 30 tickets a day for 4 campuses: account lockouts, MFA enrollment, Chromebook repairs and classroom projectors.

EDUCATION

B.S. Cyber Security · The University of Texas at San Antonio — May 2018

SKILLS

SIEM & SOAR: Splunk Enterprise Security, Splunk SOAR, Microsoft Sentinel, IBM QRadar

Endpoint & Identity: CrowdStrike Falcon, Microsoft Defender for Endpoint, Entra ID, Proofpoint

Analysis: SPL, KQL, Wireshark, Tenable, MITRE ATT&CK, PowerShell, Python

CERTIFICATIONS

CompTIA Security+ · CompTIA CySA+ · GIAC Certified Incident Handler (GCIH)