Renee Hollis

Round Rock, TX · renee.hollis@example.com · (512) 555-0190 · linkedin.com/in/example-renee-hollis

My Key Qualifications

- **5 years in cybersecurity** across incident response, detection tuning, and vulnerability management, from Simmons Bank SOC in 2021 to AvidXchange today.
- **Splunk detection engineering**: tuned suspicious-authentication and persistence detections, cutting false positives from 94 alerts per week to 51.
- **27 medium-severity incidents led and contained** for phishing and account compromise at AvidXchange, median MTTR 2.6 hours.
- Vulnerability management with **Tenable**: critical-findings remediation within SLA raised from 71% to 89% using CVSS and asset-criticality prioritization.
- **AWS security review** with cloud engineering: closed 14 configuration gaps across CloudTrail, GuardDuty, Security Hub, and IAM in two quarters.
- Operational reporting with **MTTD, MTTR, and patch-compliance dashboards** in Splunk and SQL, cutting weekly reporting from 3 hours to 50 minutes.
- **PCI DSS and SOC 2 audit support** in fintech and regulated banking environments; CompTIA CySA+ certified.

Experience

Cyber Security Analyst — **AvidXchange**, a fintech company providing accounts payable automation and payment software

May 2023 – Present · 3 yrs 6 mos

- Investigate security events across cloud, endpoint, and identity environments, correlating evidence from Splunk, CrowdStrike, Okta, and AWS telemetry.
- Tuned Splunk detections for suspicious authentication, impossible travel, and endpoint persistence activity, cutting false positives from 94 alerts per week to 51 by rewriting search logic and adding Okta and CrowdStrike context.
- Led response for medium-severity phishing and account compromise investigations, containing 27 incidents in 2025 with a median MTTR of 2.6 hours by correlating email, identity, and endpoint evidence and coordinating containment with IT.
- Built a risk-based vulnerability management workflow for Tenable findings, prioritizing by CVSS, exploitability, and asset criticality and tracking action items in Jira, which raised critical vulnerability remediation within SLA from 71% to 89%.
- Partnered with cloud engineering to review AWS logging and security guardrails, closing 14 configuration gaps across CloudTrail, GuardDuty, Security Hub, and IAM in two quarters.
- Created Splunk and SQL dashboards for MTTD, MTTR, and patch compliance metrics, cutting weekly security reporting preparation from 3 hours to 50 minutes, and supported evidence collection for PCI DSS and SOC 2 audits.

Sample resume made with Specific Resume · specificresume.com

Security Operations Analyst — **Simmons Bank**, a regional consumer and commercial bank

Nov 2021 – Apr 2023 · 1 yr 5 mos

- Investigated endpoint, identity, and network alerts across Splunk, CrowdStrike, and Okta, closing an average of 22 security cases per week with documented disposition and evidence, and escalating higher-risk incidents under runbooks.
- Improved the phishing review process for user-reported emails by standardizing triage notes, response categories, and mailbox routing, cutting duplicate analyst handling by 31% over 6 months.
- Supported quarterly vulnerability remediation reporting from Tenable scans, validating asset ownership and exposure and following up on open tickets, cutting high-risk findings older than 30 days from 58 to 33.

Education

- **University of Arkansas at Little Rock** — Bachelor of Science in Information Science · 2017 – 2021

Skills

- **Security Operations & Response:** Incident Response, Detection Engineering, Splunk, CrowdStrike, Okta
- **Cloud Security:** AWS, CloudTrail, GuardDuty
- **Vulnerability & Compliance:** Vulnerability Management, Tenable, PCI DSS Control Support, Jira

Certifications

- **CompTIA CySA+** – CompTIA (2024)