Betty Harris

Cybersecurity

Cybersecurity lead with 14 years across regulated industries, currently running detection and response for a publicly traded medical device company. Builds programs that survive audits and real attackers, with a focus on hiring, mentoring, and measurable risk reduction.

Minneapolis, MN 12345

(612) 555-0199

darnell.boateng@example.com

KEY SKILLS

- Detection engineering and SOC operations leadership
- Incident response and breach coordination
- Threat intelligence program development
- SIEM platforms (Splunk, Sentinel) and EDR (CrowdStrike, SentinelOne)
- OT and ICS security (Dragos, NERC CIP)
- Medical device security and FDA premarket cybersecurity guidance
- PCI DSS, HIPAA, SOX, and NERC compliance programs
- Threat modeling and product security partnerships
- Identity threat detection and response (ITDR)
- Team building, hiring, and analyst mentorship
- Board and executive-level security reporting
- Tabletop exercise design and crisis communications

PROFESSIONAL EXPERIENCE

HEAD OF DETECTION AND RESPONSE | HALDEN MEDICAL SYSTEMS, MINNEAPOLIS, MN
2021 – PRESENT

- Lead a team of 11 analysts and engineers across SOC, threat intel, and detection engineering covering 28,000 employees and 4 manufacturing sites.
- Cut average dwell time from 19 days to 3 days over two years by combining EDR rollout, identity threat detection, and a 24/7 follow-the-sun model.
- Owned response on a third-party software supply chain incident affecting two product lines and briefed the board within 48 hours.
- Rebuilt the on-call rotation and burnout policy after losing three analysts in 2022; voluntary attrition has been zero in the last 14 months.
- Partner with product security on threat modeling for next-gen insulin pumps under FDA premarket cybersecurity guidance.

SOC MANAGER | GREATLAKES ENERGY COOPERATIVE, ST. PAUL, MN
2017 – 2021

- Built the SOC from two analysts to a 24/7 team of nine covering generation, transmission, and corporate IT.
- Implemented NERC CIP-required logging and access reviews across 17 substations, passed two audits without findings.
- Stood up an OT-specific detection layer using Dragos and integrated alerts into the existing Splunk workflow.
- Created a security apprenticeship program with the local community college; six of nine current analysts came through it.

LEAD SECURITY ENGINEER | NORTHGATE RETAIL HOLDINGS, BLOOMINGTON, MN
2014 – 2017

- Led tokenization and PCI scope reduction project across 412 store locations, removing card data from store servers entirely.
- Built the company's first threat intel function and feed integrations into the SIEM.
- Coordinated response on a POS malware incident, including external counsel, card brand notifications, and forensic vendor management.

- Trained store IT managers on incident reporting and ran annual phishing simulations across 9,800 employees.

SENIOR SECURITY ANALYST | CITADEL BANK OF THE PLAINS, OMAHA, NE
2011 – 2014

- Investigated fraud-linked malware on customer endpoints and partnered with the FBI Cyber Task Force on two cases.
- Owned IDS and DLP tuning across the corporate network and online banking platform.
- Wrote the bank's first incident response plan, approved by examiners during the next OCC exam.
- Mentored two analysts who later moved into the bank's threat intel team.

EDUCATION

- M.S. Information Security, Carnegie Mellon University, 2013
- B.S. Computer Science, University of Nebraska-Lincoln, 2010
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Detection Analyst (GCDA)
- CISSP, ISC2, active since 2015