

Betty Harris

Cyber Security Analyst

Raleigh, NC 12345 | (919) 555-0101 | priya.ramaswamy@example.com

Cybersecurity analyst with 5 years in 24/7 security operations across fintech and healthcare. Strong in Splunk detection engineering, endpoint alert triage on CrowdStrike and SentinelOne, and phishing response. Comfortable working incidents end-to-end and writing the postmortem that keeps them from repeating.

Professional Experience

CYBERSECURITY ANALYST II | MERIDIAN FINANCIAL TRUST, RALEIGH, NC | 2022 – PRESENT

- Own escalated alerts from the Tier 1 queue: business email compromise attempts, suspicious OAuth grants, and endpoint detections routed out of CrowdStrike Falcon.
- Rewrote 14 noisy Splunk correlation rules that were generating ~600 false positives a week, cutting alert volume by roughly 40% without missing a confirmed incident in the following two quarters.
- Led the response on a credential-stuffing burst against the customer portal; blocked source ASNs at the web application firewall, forced password resets on 2,300 accounts, and drafted the customer notification with legal.
- Author of the phishing playbook the SOC now uses, including a Sentinel hunt template for OAuth consent phishing in Microsoft 365.

SOC ANALYST | KETTLEWOOD HEALTH SYSTEMS, DURHAM, NC | 2020 – 2022

- Triaged 40-60 alerts per shift out of Microsoft Sentinel, focusing on lateral movement patterns and unusual service account activity on the EHR network.
- Escalated the first sign of a ransomware precursor (Cobalt Strike beacon on a radiology workstation) to the incident response team within 12 minutes; host was isolated before encryption.
- Built dashboards for the security chief's weekly report tracking mean time to acknowledge, mean time to contain, and top alert sources.
- Ran quarterly tabletop exercises with the help desk on phishing escalation paths.

Education

B.S. Information Systems, North Carolina State University, 2020

CompTIA Security+ (2020), CompTIA CySA+ (2022), GIAC Security Essentials (2023)

Key Skills

- Splunk search language and detection engineering
- CrowdStrike Falcon, SentinelOne
- Adversary technique mapping
- Python and PowerShell for triage automation
- M365 security (Defender, Purview)
- Microsoft Sentinel query authoring
- Phishing analysis (headers, sandboxing, URL detonation)
- Incident response and chain-of-custody notes
- Wireshark and Zeek
- Threat intel enrichment with VirusTotal and shared indicator platforms