

BC

Benjamin Collins

Cybersecurity

Cybersecurity analyst with six years protecting fintech and healthcare environments. Strong in SIEM tuning, incident response, and cloud workload security across AWS and Azure. Recent focus on detection engineering and reducing alert fatigue for tier-1 SOC teams.

CONTACT INFORMATION

 (919) 555-0142

 priya.raman@example.com

 Raleigh, NC 12345

KEY SKILLS

- SIEM: Splunk, Microsoft Sentinel
- EDR: CrowdStrike Falcon, SentinelOne
- Cloud security: AWS GuardDuty, Azure Defender
- Incident response and forensics
- MITRE ATT&CK detection engineering
- Vulnerability management (Tenable, Qualys)
- Python and KQL scripting
- Identity: Okta, Active Directory
- Phishing analysis and email security

PROFESSIONAL EXPERIENCE

SENIOR SECURITY ANALYST | BEACON LEDGER FINANCIAL, RALEIGH, NC 2022 – PRESENT

- Tuned Splunk correlation rules and dropped false-positive volume from roughly 9,400 to 2,180 alerts per week, freeing two analysts for threat hunting.
- Led containment on a credential-stuffing incident affecting 14 customer accounts; coordinated with fraud team and closed the case in under six hours.
- Built detection content for MITRE ATT&CK techniques T1078 and T1566, mapped to existing log sources in CrowdStrike and Okta.
- Partnered with cloud engineering to roll out AWS GuardDuty across 43 accounts and standardized response runbooks for each finding type.
- Mentored two junior analysts through Security+ prep and weekly tabletop exercises.

SECURITY ANALYST II | NORTHWIND HEALTH SYSTEMS, DURHAM, NC 2019 – 2022

- Investigated phishing and malware tickets in a 24/7 SOC covering 11,000 endpoints, averaging around 35 cases per week.
- Owned vulnerability remediation tracking in Tenable, working with infra teams to close critical CVEs within the 14-day SLA.
- Drafted the hospital's first ransomware playbook after a regional peer was hit; ran two tabletop exercises with IT leadership.
- Reviewed firewall change requests and flagged risky rules before deployment, catching about one misconfiguration per week.

EDUCATION

B.S. in Information Technology, North Carolina State University, 2019

Certifications: CompTIA Security+, GIAC GCIH, AWS Certified Security - Specialty