



Michael Harris

Cyber Security Analyst

Tier 2 analyst with 4 years of incident response and detection engineering across retail and SaaS environments. Focus on cloud-native threats in Amazon and Microsoft 365 estates, plus writing detections that survive contact with production.

CONTACT INFORMATION



(612) 555-0103



elena.vosko@example.com



Minneapolis, MN 12345

EDUCATION

- **B.S. COMPUTER SCIENCE, UNIVERSITY OF MINNESOTA, 2021**
- **GIAC SECURITY ESSENTIALS, 2023**
- **CERTIFIED ETHICAL HACKER, 2024**

KEY SKILLS

- **Microsoft Sentinel detection writing**
- **SentinelOne, CrowdStrike Falcon**
- **CloudTrail, GuardDuty, and cloud identity investigation**
- **Sigma rule authoring**
- **Python for security automation**
- **Cloud adversary technique mapping**
- **Business email compromise response**
- **Purple team exercise participation**
- **Elastic and Kibana**
- **Threat intel platforms including Anomali**

PROFESSIONAL EXPERIENCE

TIER 2 SOC ANALYST I NORTHLAKE RETAIL GROUP, MINNEAPOLIS, MN | 2023 - PRESENT

- Investigate escalations for the North America SOC covering 38,000 endpoints and a mid-size Amazon cloud footprint; typical caseload is 8-12 open incidents at a time.
- Wrote a Sentinel analytics rule for anomalous multi-factor prompt-fatigue patterns that has caught 3 confirmed account takeover attempts against seasonal contractor accounts.
- Ran point on a business email compromise investigation involving a compromised vendor mailbox; recovered the transaction workflow and coordinated the \$184,000 wire recall through treasury and the bank.
- Mentor two Tier 1 analysts, reviewing their escalation write-ups weekly and running monthly detection-writing sessions.

SOC ANALYST I HALCYON DATA CLOUD, SAINT PAUL, MN | 2021 - 2023

- Triageed endpoint alerts from SentinelOne across a Linux-heavy Kubernetes environment and wrote enrichment queries against Elastic for container runtime events.
- Built a Python tool that parsed CloudTrail for suspicious role assumptions and posted findings into the SOC Slack channel; the tool caught two red-team paths during a purple team exercise.
- Handled on-call rotation once every six weeks, including one 2 a.m. page for exposed S3 credentials committed to a public repo.
- Contributed detections to the team's Sigma repo, mostly around cloud persistence techniques.