

Gary Mitchell

Cyber Security Analyst

Tempe, AZ 12345 | (480) 555-0102 | marcus.delacroix@example.com

Entry-level SOC analyst with a year of monitoring experience through a managed security provider and hands-on lab work in Splunk, Sentinel, and Wireshark. Comfortable working rotating shifts, following runbooks, and escalating cleanly.

PROFESSIONAL EXPERIENCE

Tier 1 SOC Analyst | 2024 – Present
Ironvale Managed Security, Tempe, AZ

- Monitor alerts across 22 client tenants in Splunk Enterprise Security during the overnight shift, averaging around 75 alerts reviewed per shift.
- Follow client-specific runbooks for phishing, failed remote-access logins, and endpoint detections; escalate to Tier 2 with a written summary including host, user, indicators, and initial containment step.
- Enrich alerts using VirusTotal, AbuseIPDB, and the internal asset inventory before deciding true positive vs. benign.
- Contributed 6 net-new phishing indicators to the shared threat intel platform last quarter.

EDUCATION

B.S. Cybersecurity, Arizona State University, 2024

CompTIA Security+ (2023), CompTIA Network+ (2023)

TryHackMe SOC Level 1 path completed

KEY SKILLS

- | | |
|---|---|
| • Splunk Enterprise Security (searches, dashboards) | • Microsoft Sentinel basics |
| • Phishing triage (header analysis, URL sandboxing) | • Wireshark and basic packet capture review |
| • Adversary technique framework familiarity | • Ticketing (ServiceNow, Jira) |
| • Windows and Linux fundamentals | • Basic Python scripting |