JULIAN MERCER

SECURITY OPERATIONS CENTER ANALYST

San Francisco, CA | (415) 555-0148 | julian.mercer@email.com | linkedin.com/in/julianmercer

PROFESSIONAL SUMMARY

Security Operations Center Analyst with 5+ years in 24x7 SOC environments handling SIEM alerts, threat triage, and incident escalation. Known for accurate severity calls, tight handoffs, and detection feedback that reduces analyst noise.

PROFESSIONAL EXPERIENCE

SOC Analyst II Feb 2023 - Present
CrowdStrike, Austin, TX

- Triaged 90+ daily SIEM and EDR alerts on rotating shifts, meeting a 15-minute initial-response target 96% of the time.
- Investigated confirmed intrusions using host, DNS, and proxy evidence, escalating nine incidents with complete timelines.
- Authored 17 detection tuning requests from recurring false positives, reducing weekly analyst alert volume 29%.
- Wrote shift-handoff templates and runbooks for ransomware and credential-theft alerts adopted across three SOC teams.
- Trained six new analysts on triage workflow and evidence standards, shortening their onboarding to independent shifts by two weeks.
- Mapped 25 recurring alert types to MITRE ATT&CK techniques, helping detection engineers prioritize coverage gaps for the next quarter.
- Ran monthly threat-hunting sessions on unusual PowerShell and login activity, surfacing three misconfigured service accounts for remediation.

SOC Analyst I Jun 2021 - Jan 2023
Mandiant, Reston, VA

- Monitored Splunk and Sentinel queues for managed-defense customers, escalating validated threats with clear impact statements.
- Enriched indicators with threat-intelligence feeds, improving true-positive classification accuracy to 91% in QA reviews.
- Documented 60+ closed investigations in the case system, passing 98% of internal quality audits.
- Collaborated with customer IT teams on containment steps, helping isolate compromised endpoints in under 30 minutes.
- Wrote customer-facing incident summaries for 20 managed-defense accounts, earning positive review notes on clarity from two client security leads.
- Triaged phishing reports from customer mailboxes, analyzing 150 messages and sending confirmed indicators to detection engineers.
- Documented repeatable triage steps for common login-anomaly alerts, cutting escalations that lacked evidence by about 20%.

CORE SKILLS

SIEM triage | Splunk | Microsoft Sentinel | EDR investigation | Threat intelligence | Incident escalation | Phishing analysis | Log correlation | MITRE ATT&CK | Runbook writing | Shift handoffs | DNS and proxy analysis | Detection tuning | Case documentation

EDUCATION

B.S. in Cybersecurity, George Mason University, Fairfax, VA

CERTIFICATIONS

CompTIA CySA+ | Splunk Core Certified User