Oskar Brennan

SOC Analyst (Tier 2)

Columbus, OH · oskar.brennan@example.com · (614) 555-0158 · LinkedIn · GitHub

SUMMARY

SOC analyst with 3 years on rotating 12-hour shifts across MSSP and in-house security operations, working in Microsoft Sentinel, Splunk and SentinelOne. Cut median triage time from 22 to 8 minutes with KQL enrichment queries and keep a 94% acceptance rate on escalations to incident response. Holds CompTIA CySA+ and Blue Team Level 1.

EXPERIENCE

SOC Analyst, Tier 2 — Larkspur Freight Lines

Columbus, OH · Mar 2024 – Present

- Handle Tier 2 investigations for a 24/7 SOC covering 3,800 endpoints and 14 distribution centers, closing an average of 30 escalated cases per week.
- Wrote 18 KQL enrichment queries in Microsoft Sentinel that attach user, host and geo context to each alert, cutting median triage time from 22 to 8 minutes.
- Traced an impossible-travel alert to a token theft on a dispatcher's mailbox, revoked 4 active sessions and blocked an inbox rule forwarding invoices within 35 minutes.
- Retired or rewrote 27 noisy analytics rules after a 90-day review, lowering weekly alert volume by 41% without losing coverage of any mapped ATT&CK technique.
- Mentor 4 Tier 1 analysts on case notes and escalation criteria, raising first-pass escalation acceptance from 71% to 94% over two quarters.

SOC Analyst, Tier 1 — Bluecairn Managed Defense

Dublin, OH · Jun 2022 – Feb 2024

- Monitored Splunk and SentinelOne consoles for 22 client environments, triaging around 160 alerts per 12-hour shift against client-specific runbooks.
- Spotted a living-off-the-land PowerShell pattern on a dental chain's server and escalated it with full process trees, leading to containment before any data left the network.
- Built a shared phishing-triage checklist used by 11 analysts, reducing reopened phishing tickets from 15% to 4% within 6 months.

SKILLS

SIEM & EDR: Microsoft Sentinel (KQL), Splunk (SPL), SentinelOne, Microsoft Defender for Endpoint

Investigation methods: Alert triage, email header analysis, process tree review, MITRE ATT&CK mapping, IOC pivoting

Tooling: ServiceNow SecOps, VirusTotal, URLScan, CyberChef, basic Python for log parsing

Logs and protocols: TCP/IP, DNS, Windows event logs, Entra ID sign-in logs, NIST 800-61 incident handling

CERTIFICATIONS

CompTIA CySA+, 2024

Blue Team Level 1 (BTL1), 2023

EDUCATION

B.S. Cybersecurity and Information Assurance, Franklin University, 2022

Fictional example by FindAJobAI: the person, employers and numbers are invented.