Cybersecurity Analyst

(555) 010-0000 · you@example.com · City, ST · linkedin.com/in/your-name

SUMMARY

Cybersecurity analyst with five years in security operations, skilled in Splunk and Microsoft Sentinel, focused on threat detection, incident response, and vulnerability management aligned to the NIST and MITRE ATT&CK frameworks.

EXPERIENCE

Cybersecurity Analyst, Tier 2 SOC, Sentinel Security Operations 2021 – Present
City, ST

- Triaged roughly 450 SIEM alerts per week in Splunk, cutting false positives 46% by tuning correlation rules.
- Reduced mean time to detect from 38 minutes to 11 by building 25 ATT&CK-mapped detection use cases.
- Led containment on 60-plus security incidents with zero confirmed data exfiltration over two years.
- Ran a phishing-simulation program that lowered employee click-through from 18% to 4% across 1,400 staff.
- Remediated 320 high-severity vulnerabilities on a quarterly cycle, keeping the critical backlog at zero.
- Authored 15 incident-response runbooks that cut average response handoff time roughly in half.
- Investigated and closed a credential-stuffing campaign, blocking 12,000 malicious login attempts.

Security Operations Analyst, Cascade Information Security 2019 – 2021
City, ST

- Monitored a Microsoft Sentinel SIEM covering 3,000 endpoints across a hybrid cloud environment.
- Cut endpoint malware detections 33% by deploying and tuning CrowdStrike EDR policies.
- Ran weekly vulnerability scans with Nessus and prioritized fixes using CVSS scoring.
- Investigated 200-plus tier-1 alerts monthly, escalating only true positives to incident response.
- Built dashboards that gave leadership a live view of open findings and patch compliance at 94%.
- Documented access reviews that supported a clean SOC 2 audit with no security findings.

EDUCATION

Bachelor of Science in Cybersecurity 2015 – 2019
State University — City, ST

CERTIFICATIONS & LICENSES

CompTIA Security+ · GIAC Certified Incident Handler (GCIH)

SKILLS

SIEM (Splunk) · Microsoft Sentinel · Incident response · MITRE ATT&CK · Vulnerability management · EDR (CrowdStrike) · Threat hunting · NIST framework · Phishing defense · Log analysis · Security documentation · Network security basics