Daniel Kowalski

Cybersecurity Analyst

Pittsburgh, PA · daniel.kowalski@example.com · (412) 555-0162 · LinkedIn · GitHub

SUMMARY

Cybersecurity analyst with 4 years of experience in healthcare IT and managed security services, working in Splunk, CrowdStrike and Qualys. Led the containment of a phishing-driven credential compromise affecting 40 accounts within 2 hours of detection, and cut false-positive alerts by 35% through tuned correlation rules. Comfortable owning incident response from detection to post-mortem.

EXPERIENCE

Cybersecurity Analyst — Meridian Health Systems

Pittsburgh, PA · Feb 2023 – Present

- Monitor and triage alerts in Splunk ES for a network covering 12 hospital and clinic locations, investigating an average of 25 incidents a week.
- Led containment of a phishing-driven credential compromise affecting 40 accounts, isolating affected endpoints and resetting credentials within 2 hours of detection.
- Tuned 60 SIEM correlation rules against 6 months of alert history, cutting false positives by 35% and freeing time for deeper investigation.
- Ran monthly vulnerability scans across 900 endpoints with Qualys, prioritizing and tracking remediation of 18 critical CVEs to closure within SLA.
- Wrote and tested 5 incident response playbooks aligned to NIST 800-61, used by the on-call team during 3 real incidents last year.

SOC Analyst — Ironclad Managed Security

Pittsburgh, PA · Aug 2021 – Jan 2023

- Monitored security events for 15 client environments in CrowdStrike and Splunk, escalating 8 confirmed incidents to Tier 2 in a 15-month period.
- Investigated a ransomware precursor on a client endpoint, isolating the host and preventing lateral movement before encryption began.
- Documented and closed out 400+ Tier 1 tickets with root cause notes, maintaining a 98% SLA compliance rate.

SKILLS

Detection & response: Splunk ES, CrowdStrike Falcon, incident response, log analysis, MITRE ATT&CK

Vulnerability management: Qualys, Nessus, patch prioritization, CVSS scoring

Network & systems: TCP/IP, firewalls (Palo Alto), Windows and Linux administration, Active Directory

Frameworks: NIST 800-61, NIST CSF, basic familiarity with HIPAA security requirements

CERTIFICATIONS

CompTIA Security+

Splunk Core Certified User, 2022

EDUCATION

B.S. Information Technology, Pennsylvania State University, 2021

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