JOHN DANKO

SOC ANALYST

Greater Philadelphia | Open to Relocation | 610-724-7640 | john.g.danko@gmail.com
linkedin.com/in/john-danko-cyber | github.com/john-danko-cyber | john-danko.netlify.app

SUMMARY

Cybersecurity graduate (B.S. Computer Information Science, Cum Laude) pursuing an SOC Analyst role, with hands-on practice in **SIEM, log analysis, network traffic analysis, and incident response**. DoD Cyber Sentinel Skills Challenge competitor with hands-on Splunk and Google SecOps lab experience and published security projects on GitHub.

EDUCATION

Gwynedd Mercy University, Gwynedd Valley, PA **Fall 2024**

B.S. Computer Information Science, Cybersecurity Specialization | GPA: 3.59, Cum Laude, Dean's List

Relevant Coursework: Computer Forensics, Cybersecurity, Cybercrime, Networking Administration & Security, Operating Systems, Auditing IT, Algorithms and Data Structures

PROJECTS

Malware Incident Response Case Study **Fall 2026**

- Investigated a real DLL-sideloading infection on a personal Windows PC, tracing suspicious processes, outbound connections, and Run key and scheduled task persistence.
- Contained the incident by stopping processes, quarantining files, removing persistence, and documenting SHA256 hashes and lessons learned.
- Found that Defender alerts marked as resolved had left both programs running for 12 more days, and traced likely entry to a ClickFix fake-captcha command.

SOC Incident Response Playbook **Fall 2026**

- Wrote original SOC playbooks for phishing, malware, brute-force, ransomware, and suspicious login alerts, each following eight phases from preparation to lessons learned.
- Defined triage fields and escalation guidance so an analyst can pick up any alert type and know what to do next.

Internal Security Audit **Fall 2026**

- Audited a fictional company's security controls and compliance, finding gaps in access control, encryption, backups, and IDS, and ranked fixes by risk.
- Found missing least privilege, separation of duties, password management, and a disaster recovery plan.

DNS and ICMP Traffic Analysis **Fall 2026**

- Analyzed a provided tcpdump log from a lab scenario and traced failed website access to DNS queries returning "udp port 53 unreachable" errors.
- Showed that the DNS service, not the server host, was failing across three repeated queries, and mapped the failure to the TCP/IP model.

SYN Flood Attack Analysis **Fall 2026**

- Reviewed a provided Wireshark TCP/HTTP log and identified a SYN flood DoS attack from a single IP, then wrote an incident report on its impact.
- Found that 139 of 173 packets were attacker SYN requests, followed by RST and HTTP 504 errors for visitors.

TECHNICAL SKILLS

Tools: Splunk, Google Security Operations, Microsoft Defender, Wireshark, tcpdump, Nmap, Nessus, Metasploit, Burp Suite, FTK Imager, Autopsy, John the Ripper, pfSense

Security Operations: Incident Response Lifecycle, Alert Triage, Malware Triage, Persistence Analysis, Phishing Response, Playbook Writing, Incident Documentation, Digital Forensics, Threat Intelligence, Vulnerability Assessment

Network Analysis: Network Traffic Analysis, tcpdump/Wireshark Packet Analysis, SYN Flood/DoS Detection, TCP/IP, OSI Model, DNS/ICMP, Ports & Protocols, Firewalls, VPNs, Subnetting

Governance & Scripting: NIST SP 800-61, NIST CSF, CIA Triad, Security Auditing, Risk Assessment, Access Control/Least Privilege, Python, Bash, SQL, Linux, Windows

WORK EXPERIENCE

Server, Revolution Chop House at Valley Forge Casino, King of Prussia, PA **Fall 2022 – Present**