FELIX NARODITSKIY

Warminster, PA | (267) 264-9244 | fnaroditskiy@gmail.com
linkedin.com/in/felix-naroditskiy | felixnaroditskiy.com

SUMMARY

Cybersecurity and IT professional, CompTIA Security+ certified, with hands-on lab depth in digital forensics, incident response, malware analysis, and blue-team security operations (SIEM, IDS, packet and log analysis), plus professional experience in security governance, privacy compliance, control assessments, and AI governance. Seeking a security analyst, SOC, incident response, or GRC role.

EDUCATION

B.S. Cybersecurity Analytics and Operations – Summa Cum Laude August 2023 – May 2026
Pennsylvania State University, Abington

WORK EXPERIENCE

Cybersecurity Specialist August 2024 – Present
Stemuli – Dallas, TX (Remote)

- Lead a company-wide security program build-out: ran a NIST CSF 2.0 gap assessment across all six functions, prioritized findings in authentication, client-side data handling, and input validation into an engineering remediation queue, and built the policy and controls roadmap.
- Own COPPA/FERPA and AI governance for a K-12 platform, translating regulatory change into engineering acceptance criteria for PII blocking, age gating, and parental consent, and defining data-handling requirements for third-party AI vendors.
- Conduct recurring security control and tool reviews across the company's cloud and SaaS platforms, delivering hardening recommendations (encryption, IAM least privilege, MFA, access reviews, logging), and analyze inbound vendor and school-district security questionnaires.
- Architected segmented, identity-verified access for the student research community, coordinate user-acceptance testing of the AI-driven platform, and automate recurring reporting and review workflows using Zapier, Power Automate, and AI-assisted analysis.

Cybersecurity and Technology Intern September 2023 – August 2024
Stemuli – Dallas, TX (Remote)

- Conducted security reviews of AWS RDS, GCP, Azure, and SaaS platforms, assessing encryption at rest and in transit, IAM configuration, and compliance posture; compiled results into a reusable internal review library.
- Built team-specific security onboarding handbooks and a multi-domain employee training handbook, and proposed data governance procedures aligned with CIS, NIST, COPPA, and FERPA under Zero Trust.

Technology and Computer Hardware Intern June 2020 – August 2023
FEBA, LLC – Pipersville, PA

- Provided direct end-user technical support in a small-business environment, diagnosing and resolving hardware and software issues and walking users through fixes to minimize downtime.
- Supported, set up and configured Windows systems including operating system installation, software installation and patching, and printer and peripheral setup; performed hardware troubleshooting, repair and component replacement; supported VoIP phone systems and small-office networking including routers, Wi-Fi and cabling.

SKILLS AND CERTIFICATIONS

- **Security Operations:** SIEM & Log Analysis, IDS/IPS, Alert Triage, Incident Response, Digital Forensics, Malware Analysis, Packet Analysis, Vulnerability Assessment, Network Security, Cloud Security, IAM, Zero Trust, AI-Assisted Analysis
- **Tools:** Splunk, Elastic Stack (ELK), Snort, OSSEC, Wireshark, tcpdump, Nmap, Metasploit, OWASP ZAP, Volatility, Autopsy, FTK Imager, PeStudio, ProcMon, Active Directory, Linux, Git, Zapier, Power Automate
- **Governance & Compliance:** GRC, NIST CSF 2.0 / RMF, ISO 27000, CIS Controls, MITRE ATT&CK, COBIT 2019, Privacy Compliance (COPPA/FERPA), AI Governance, Vendor Risk, Risk Assessment, Security Control Assessments
- **Languages & Certifications:** Python, Bash, PowerShell, SQL, Java, JavaScript | CompTIA Security+; Microsoft SC-900, AZ-900, DP-900

PROJECTS

Forensic Analysis Labs (Network, Memory, Image & Log) – Identified a malicious process masquerading as a legitimate binary in a 6.4 GB memory image (Volatility), reconstructed an anti-forensic timeline from a disk image (Autopsy, FTK Imager), and wrote a Python parser for 78,000+ Windows Security Log events surfacing off-hours logons and audit-log clearing.

Capstone Forensic Ransomware Investigation – Analyzed 12.7M+ packets, 7 memory captures, 6 disk images, and 90,000+ log entries to reconstruct a four-day attack chain from phishing-based initial access through lateral movement to suspected exfiltration.

Malware Research and Analysis – Static and dynamic analysis of 12 samples in an isolated FlareVM lab, co-leading six to determine family attribution, C2 behavior, and evasion techniques.

Ransomware Incident Response Playbook – Co-authored an enterprise IR playbook mapped to NIST RMF, COBIT 2019, and MITRE ATT&CK, with NCISS severity scoring driving role-based escalation and chain-of-custody procedures.

Elderly Tech Support Fraud Risk Analysis – Scored six risks on likelihood and impact for a $1M+ tech-support fraud scenario, modeling the scam as a serial-dependency system with defined interdiction points and recommending a defense-in-depth mitigation strategy.