FOTIOS NANOS
Cybersecurity Analyst | Ready to Deploy
📧 fotis.nanos.sec@gmail.com | 🔗 linkedin.com/in/fotisnanos | 💻 fotisnanossec.github.io
📍 Vienna, Austria & Athens, Greece | EU Citizen | Multilingual (Greek/English/German)

PROFESSIONAL SUMMARY

SOC Level 1 certified cybersecurity analyst with comprehensive incident response capabilities and unique analytical background. Demonstrated expertise through top 2% global TryHackMe ranking and official "Datensicherheitsspezialist" assessment. Combines systematic methodology from classical music training with hands-on security operations experience. Ready for immediate deployment with proven investigation skills, advanced threat analysis, and enterprise security understanding.

KEY ACHIEVEMENTS

🎯 SOC Level 1 Path - 100% Complete (TryHackMe, September 2025)
🏆 Top 2% Global Ranking - 155+ rooms completed, 25+ rare badges
🏛️ Official Assessment - "Datensicherheitsspezialist" with "sehr gute Kenntnisse" (BEST Institut Vienna)
⚡ SAL1 Certification Ready - Eligible for Security Analyst Level 1 professional certification
🚀 Advanced Incident Response - Complete Boogeyman series analysis with professional documentation

CORE TECHNICAL CAPABILITIES

Incident Response & Investigation

- End-to-end incident analysis: email forensics → malware analysis → network reconstruction
- Memory forensics with Volatility 3: process analysis, persistence detection, C2 identification
- PowerShell forensics: log analysis, obfuscation techniques, attack chain reconstruction
- Multi-stage attack investigation: spear phishing, lateral movement, domain compromise

Network & Traffic Analysis

- PCAP analysis with Wireshark/tshark: protocol analysis, anomaly detection, data recovery
- Network forensics: DNS tunneling detection, C2 communication analysis, traffic correlation
- Threat hunting: IOC identification, behavioral analysis, pattern recognition
- Protocol analysis: HTTP/HTTPS, DNS, TCP/UDP deep packet inspection

Malware & Threat Analysis

- Static analysis: file signatures, metadata examination, hash verification
- Dynamic analysis: sandbox execution, behavioral analysis, persistence mechanisms
- Document analysis: macro extraction (olevba), embedded payload identification
- Threat intelligence: IOC correlation, TTPs mapping, campaign attribution

Security Tools Proficiency

- SIEM Platforms: Splunk operations, ELK stack analysis, log correlation
- Forensic Tools: KAPE, Redline, Autopsy, lnkparse, Volatility 3
- Network Tools: Nmap, Snort, Wireshark, tshark, Zeek, Brim
- Analysis Tools: jq, grep, xxd, PowerShell, Python scripting

CYBERSECURITY PROJECTS

🔍 Advanced Incident Response Portfolio | Multi-Stage Attack Analysis
- Complete Boogeyman series investigation (3 sophisticated scenarios)
- DNS exfiltration recovery, memory forensics, Windows log analysis
- Professional documentation demonstrating enterprise-level investigation skills
- GitHub: fotisnanossec.github.io/blog/

⚙️ Domain Analyzer | Automated Threat Intelligence
- Python-based reconnaissance tool with API integration and LLM analysis
- Automated security reporting and intelligence correlation
- Demonstrates automation, threat intelligence, and report generation capabilities

🛡️ Vulnerability Assessment Suite | Security Scanning Integration
- Integrates Nmap, Nikto, SQLMap with automated report generation
- Professional security assessment documentation
- Showcases vulnerability assessment and technical writing skills

🌐 Network Forensics Projects | PCAP Analysis Portfolio
- Comprehensive network traffic analysis demonstrating forensic capabilities
- Threat hunting through structured PCAP investigation
- Evidence of systematic analysis methodology and documentation skills

CERTIFICATIONS & TRAINING

✅ Completed
- TryHackMe SOC Level 1 Path (100% Complete, September 2025)
- Professional IT Assessment - BEST Institut Vienna (September 2025)
- Rating: "Datensicherheitsspezialist" with "sehr gute Kenntnisse"
- TryHackMe Global Ranking: Top 2% (155+ rooms, 25+ badges)

🎯 Ready for Certification
- Security Analyst Level 1 (SAL1) Professional Certification - Exam eligible

📚 In Progress
- CompTIA Security+ (Target: December 2025)
- Security Engineer Path: 13% complete
- Jr Penetration Tester Path: 22% complete

EDUCATION & BACKGROUND

Master Artium, Guitar Performance | University Mozarteum Salzburg | 2006-2010
- Developed analytical thinking, pattern recognition, and systematic methodology

Diploma, Electronics, Computer & Network Technology | TEE Athens | 1998-2002
- Foundation in computer networks, electronics, and system administration
- Early technical education providing systematic approach to complex systems

Professional Music Career | International | 2010-2025

- Applied analytical skills to complex compositions and performance challenges
- Developed discipline, attention to detail, and performance under pressure
- International collaboration across Austria, Germany, France, Greece, Argentina

DEMONSTRATED SOC ANALYST CAPABILITIES

Real-World Investigation Skills

- Complete incident response lifecycle: detection → analysis → containment → eradication
- Multi-vector attack analysis: email → document → payload → persistence → exfiltration
- Cross-platform investigation: Windows, Linux, network infrastructure
- Enterprise security understanding: Active Directory, domain controllers, lateral movement

Technical Documentation Excellence

- Professional incident reports with technical accuracy and clear methodology
- Comprehensive writeups demonstrating investigation process and findings
- Executive-level summaries with actionable recommendations
- Evidence preservation and chain of custody understanding

Threat Hunting & Analysis

- Advanced persistent threat (APT) technique recognition
- MITRE ATT&CK framework mapping and TTP analysis
- Behavioral analysis and anomaly detection
- Threat intelligence integration and IOC correlation

LANGUAGES & MOBILITY

- Greek: Native | English: Fluent (C2) | German: Professional (B2)
- EU Citizenship - No visa restrictions across European markets
- Available for immediate relocation and 24/7 shift work

UNIQUE VALUE PROPOSITION

Rare combination of systematic analytical training from classical music performance with comprehensive cybersecurity foundation. Brings disciplined methodology, pattern recognition expertise, and creative problem-solving to complex security challenges. Proven ability to work under pressure, maintain attention to detail, and communicate effectively across cultural contexts. Ready for immediate deployment with validated technical capabilities and professional assessment confirming cybersecurity expertise.

CONTACT & PORTFOLIO

📧 fotis.nanos.sec@gmail.com
🔗 LinkedIn: linkedin.com/in/fotisnanos
💻 Portfolio: fotisnanossec.github.io
🛡️ SOC Toolkit: fotisnanossec.github.io/soc-toolkit/
📊 TryHackMe: tryhackme.com/p/StygianR00t