

FOTIOS NANOS

Cybersecurity Analyst | IT-Sicherheitsspezialist | Einsatzbereit

 fotis.nanos.sec@gmail.com |  linkedin.com/in/fotisnanos |  fotisnanossec.github.io


 +43 660 502 4795 |  Wien, Österreich & Athen, Griechenland | EU-Bürger

PROFESSIONELLE ZUSAMMENFASSUNG


Zertifizierter SOC Level 1 Cybersecurity-Analyst mit umfassenden Incident-Response-Fähigkeiten und einzigartigem analytischen Hintergrund. Offiziell als "Datensicherheitsspezialist" mit "sehr gute Kenntnisse" durch BEST Institut Wien bewertet. Verbindet systematische Methodik aus klassischer Musikausbildung mit praktischer Sicherheitserfahrung. Bereit für sofortigen Einsatz mit nachgewiesenen Untersuchungsfähigkeiten und tiefem Verständnis für österreichische Geschäftskultur.


HAUPTQUALIFIKATIONEN

 SOC Level 1 Pfad - 100% Abgeschlossen (TryHackMe, September 2025)

 Top 2% Globales Ranking - 155+ Räume abgeschlossen, 25+ seltene Abzeichen

 Offizielle Bewertung - "Datensicherheitsspezialist" mit "sehr gute Kenntnisse" (BEST Institut Wien)

 SAL1 Zertifizierungs-bereit - Berechtigt für Security Analyst Level 1 Berufszertifikat

 Erweiterte Incident Response - Vollständige Boogeyman-Serie Analyse mit professioneller Dokumentation

KERN-TECHNISCHE KOMPETENZEN

Incident Response & Untersuchung

- End-to-End Incident-Analyse: E-Mail-Forensik → Malware-Analyse → Netzwerk-Rekonstruktion
- Memory-Forensik mit Volatility 3: Prozessanalyse, Persistenz-Erkennung, C2-Identifikation
- PowerShell-Forensik: Log-Analyse, Verschleierungstechniken, Angriffsketten-Rekonstruktion

- Mehrstufige Angriffs-Untersuchung: Spear-Phishing, Lateral Movement, Domain-Kompromittierung

Netzwerk & Traffic-Analyse

- PCAP-Analyse mit Wireshark/tshark: Protokollanalyse, Anomalie-Erkennung, Datenwiederherstellung
- Netzwerk-Forensik: DNS-Tunneling-Erkennung, C2-Kommunikationsanalyse, Traffic-Korrelation
- Threat Hunting: IOC-Identifikation, Verhaltensanalyse, Mustererkennung
- Protokoll-Analyse: HTTP/HTTPS, DNS, TCP/UDP Deep-Packet-Inspection

Malware & Bedrohungsanalyse

- Statische Analyse: Dateisignaturen, Metadaten-Untersuchung, Hash-Verifizierung
- Dynamische Analyse: Sandbox-Ausführung, Verhaltensanalyse, Persistenz-Mechanismen
- Dokument-Analyse: Makro-Extraktion (olevba), eingebettete Payload-Identifikation
- Threat Intelligence: IOC-Korrelation, TTPs-Mapping, Kampagnen-Attribution

Sicherheitstools-Kompetenz

- SIEM-Plattformen: Splunk-Betrieb, ELK-Stack-Analyse, Log-Korrelation
- Forensik-Tools: KAPE, Redline, Autopsy, Inkpase, Volatility 3
- Netzwerk-Tools: Nmap, Snort, Wireshark, tshark, Zeek, Brim
- Analyse-Tools: jq, grep, xxd, PowerShell, Python-Scripting

CYBERSECURITY-PROJEKTE

Erweiterte Incident Response Portfolio | Mehrstufige Angriffs-Analyse

- Vollständige Boogeyman-Serie Untersuchung (3 anspruchsvolle Szenarien)
- DNS-Exfiltration-Wiederherstellung, Memory-Forensik, Windows-Log-Analyse

- Professionelle Dokumentation demonstriert Unternehmen-Level Untersuchungsfähigkeiten
- GitHub Portfolio: fotisnanossec.github.io/blog/

Domain Analyzer | Automatisierte Threat Intelligence

- Python-basiertes Aufklärungs-Tool mit API-Integration und LLM-Analyse
- Automatisierte Sicherheitsberichterstattung und Intelligence-Korrelation
- Demonstriert Automatisierung, Threat Intelligence und Berichtserstellung

Vulnerability Assessment Suite | Sicherheits-Scanning-Integration

- Integriert Nmap, Nikto, SQLMap mit automatisierter Berichtserstellung
- Professionelle Sicherheitsbewertungs-Dokumentation
- Zeigt Schwachstellen-Assessment und technisches Schreiben

Netzwerk-Forensik-Projekte | PCAP-Analyse Portfolio

- Umfassende Netzwerk-Traffic-Analyse demonstriert forensische Fähigkeiten
- Threat Hunting durch strukturierte PCAP-Untersuchung
- Nachweis systematischer Analyse-Methodik und Dokumentationsfähigkeiten

ZERTIFIZIERUNGEN & AUSBILDUNG

Abgeschlossen

- TryHackMe SOC Level 1 Pfad (100% Abgeschlossen, September 2025)
- Professionelle IT-Bewertung - BEST Institut Wien (September 2025)
- Bewertung: "Datensicherheitsspezialist" mit "sehr gute Kenntnisse"
- TryHackMe Globales Ranking: Top 2% (155+ Räume, 25+ Abzeichen)

Zertifizierungs-bereit

- Security Analyst Level 1 (SAL1) Berufszertifikat - Prüfungsberechtigt

In Bearbeitung

- CompTIA Security+ (Ziel: Dezember 2025)
- Security Engineer Pfad: 13% abgeschlossen
- Jr Penetration Tester Pfad: 22% abgeschlossen

AUSBILDUNG & HINTERGRUND

Master Artium, Gitarren-Performance | Universität Mozarteum Salzburg | 2006-2010

- Entwickelt analytisches Denken, Mustererkennung und systematische Methodik

Diplom, Elektronik, Computer & Netzwerktechnik | TEE Athen | 1998-2002

- Fundament in Computer-Netzwerken, Elektronik und Systemadministration
- Frühe technische Ausbildung bietet systematischen Ansatz für komplexe Systeme

Professionelle Musik-Karriere | International | 2010-2025

- Angewandt analytische Fähigkeiten auf komplexe Kompositionen und Performance-Herausforderungen
- Entwickelt Disziplin, Aufmerksamkeit für Details und Performance unter Druck
- Internationale Zusammenarbeit in Österreich, Deutschland, Frankreich, Griechenland, Argentinien

NACHGEWIESENE SOC-ANALYST-FÄHIGKEITEN

Real-World Untersuchungsfähigkeiten

- Vollständiger Incident Response Lebenszyklus: Erkennung → Analyse → Eindämmung → Beseitigung
- Multi-Vektor Angriffs-Analyse: E-Mail → Dokument → Payload → Persistenz → Exfiltration
- Cross-Platform Untersuchung: Windows, Linux, Netzwerk-Infrastruktur
- Unternehmens-Sicherheitsverständnis: Active Directory, Domain-Controller, Lateral Movement

Technische Dokumentations-Exzellenz

- Professionelle Incident-Berichte mit technischer Genauigkeit und klarer Methodik
- Umfassende Writeups demonstrieren Untersuchungsprozess und Befunde
- Executive-Level Zusammenfassungen mit umsetzbaren Empfehlungen
- Nachweis-Sicherung und Chain-of-Custody Verständnis

Threat Hunting & Analyse

- Advanced Persistent Threat (APT) Technik-Erkennung
- MITRE ATT&CK Framework Mapping und TTP-Analyse
- Verhaltensanalyse und Anomalie-Erkennung
- Threat Intelligence Integration und IOC-Korrelation

ÖSTERREICH-SPEZIFISCHE QUALIFIKATIONEN

Lokale Markt-Kompetenz

- Langjährige Wien-Erfahrung mit Verständnis österreichischer Geschäftskultur
- Systematische, prozessorientierte Arbeitsweise entspricht österreichischen Standards
- Deutschkenntnisse ermöglichen effektive Kommunikation mit lokalen Teams
- Vertraut mit österreichischen Compliance-Anforderungen und Datenschutz

Unternehmens-Integration

- Bewährte Fähigkeit zur Arbeit in multikulturellen europäischen Teams
- Verständnis für österreichische Hierarchien und Entscheidungsprozesse
- Disziplinierter Ansatz passt zu österreichischen Qualitätsstandards
- Bereit für langfristige Karriereentwicklung in österreichischen Unternehmen

SPRACHEN & MOBILITÄT

- Deutsch: Professionell (B1-B2) - Kontinuierliche Verbesserung
- Englisch: Fließend (C2) - Technische und Geschäftskommunikation
- Griechisch: Muttersprache
- EU-Bürgerschaft - Keine Visa-Beschränkungen in europäischen Märkten
- Verfügbar für Wien-basierte Positionen und österreichweite Projekte

EINZIGARTIGE WERTVERSPRECHEN


Seltene Kombination aus systematischem analytischen Training von klassischer Musik-Performance mit umfassender Cybersecurity-Grundlage. Bringt disziplinierte Methodik, Mustererkennung-Expertise und kreative Problemlösung zu komplexen Sicherheits-Herausforderungen. Bewährte Fähigkeit unter Druck zu arbeiten, Aufmerksamkeit für Details zu bewahren und effektiv über kulturelle Kontexte zu kommunizieren. Bereit für sofortigen Einsatz mit validierten technischen Fähigkeiten und professioneller Bewertung, die Cybersecurity-Expertise bestätigt.


VERFÜGBARKEIT


- Sofortiger Einsatz möglich
- Wien-basiert mit Flexibilität für österreichweite Projekte
- Bereit für Vollzeit-Positionen und Schichtarbeit
- Interessiert an systematischen, prozessorientierten Arbeitsumgebungen
- Langfristige Karriereentwicklung in österreichischen Cybersecurity-Markt angestrebt


KONTAKT & PORTFOLIO

 fotis.nanos.sec@gmail.com

 LinkedIn: [linkedin.com/in/fotisnanos](https://www.linkedin.com/in/fotisnanos)

 Portfolio: fotisnanossec.github.io

 SOC Toolkit: fotisnanossec.github.io/soc-toolkit/

 TryHackMe: tryhackme.com/p/StygianR00t