Antonio De Luca

Junior Analista Cybersecurity

Napoli, Italia · antonio.deluca@gmail.com · +39 349 356 7890 ·
linkedin.com/in/antoniodeluca-security · tryhackme.com/p/antoniodeluca

Laureato Magistrale in Sicurezza Informatica all'Universita Federico II di Napoli con **110/110**. Stage di 6 mesi nel SOC di Leonardo S.p.A. con analisi di **1.200 alert/mese** e identificazione di **3 campagne di phishing** targeted. Certificazione CompTIA Security+. Top 5% TryHackMe con 480 sfide completate.

ESPERIENZA

Tirocinante SOC Analyst, Leonardo S.p.A. - Cyber Security Division, Napoli *Set 2024 – Feb 2025*

Stage di 6 mesi nel Security Operations Center di Leonardo, leader europeo nella difesa, aerospaziale e sicurezza, con clienti istituzionali e infrastrutture critiche nazionali.

- Analizzato in media **1.200 alert di sicurezza al mese** su Splunk SIEM con triage, correlazione e classificazione per priorita (P1-P4)
- Identificato **3 campagne di phishing** targeted dirette a clienti del settore difesa tramite correlazione di IOC su VirusTotal, Shodan e threat feed MISP
- Condotto **4 vulnerability assessment** su applicazioni web e infrastruttura con Nessus e OWASP ZAP: 48 vulnerabilita identificate, di cui 8 critiche (CVSS >= 9.0)
- Risposto a **12 incidenti** di sicurezza (livello P2-P3) con analisi forense su log Windows Event, Sysmon e network traffic (Zeek, Wireshark)
- Prodotto **6 threat intelligence report** mensili su campagne APT che colpivano il settore difesa europeo, distribuiti al team di 15 analisti

CTF Player e Ricercatore di Sicurezza, Team CyberNaples CTF, Napoli *Set 2022 – Ago 2024*

Membro attivo del team universitario di Capture The Flag dell'Universita Federico II.

- Partecipato a **18 competizioni CTF** nazionali e internazionali con classifiche nelle prime 50 posizioni in 8 gare
- Specializzato in challenge di Web Exploitation e Binary Exploitation con **340 flag** catturate in 2 anni

ISTRUZIONE

Titolo e specializzazione, Universita degli Studi di Napoli Federico II, Napoli *Set 2022 – Apr 2025*

Voto di laurea: **110/110**. Tesi: Tecniche di evasione degli Endpoint Detection and Response (EDR): analisi empirica su 5 prodotti leader di mercato con 8 metodologie di test.

- Corsi rilevanti: Sicurezza delle Reti, Crittografia Applicata, Malware Analysis, Penetration Testing, Diritto Informatico

COMPETENZE

Splunk SIEM, Wireshark / Zeek, Nessus / OpenVAS, Metasploit, OWASP ZAP, MISP (Threat Intelligence), Python (scripting sicurezza), Bash, Linux (Kali, Ubuntu), Windows Forensics, MITRE ATT&CK Framework, Incident Response

CERTIFICAZIONI

CompTIA Security+ (SY0-701), CompTIA *Giu 2024 – Lug 2024*

LINGUE

Italiano (madrelingua), Inglese (B2)

PROGETTI

Test di **8 tecniche** di evasione (process injection, AMSI bypass, reflective DLL loading) su 5 EDR leader (CrowdStrike, SentinelOne, Defender, Cylance, Carbon Black). **3 vulnerabilita** identificate, segnalate ai vendor tramite responsible disclosure.

REFERENZE

Dott. Raffaele Esposito, SOC Team Lead, Leonardo S.p.A. - Cyber Security, r.esposito@leonardo.com, +39 081 7790 111

ATTIVITÀ EXTRACURRICULARE

Top 5% Player - TryHackMe *Set 2021 – Apr 2025*

Piattaforma di apprendimento cybersecurity con **480 sfide** completate in Web Exploitation, Network Security, Forensics e Malware Analysis. Ranking nella top **5%** tra 2 milioni di utenti globali.

Organizzatore - CyberNaples Security Conference 2024 *Mag 2024 – Giu 2024*

Conferenza universitaria di sicurezza informatica con **8 speaker** da industria e accademia e **120 partecipanti**. Gestito la logistica e il programma dell'evento.