

Vincenzo Miccoli

Cyber Security Manager

Cyber Threat Intelligence · Incident Response · Governance (NIS2, DORA)

Taranto · Bologna · Full Remote

Sito: vincenzomiccoli.com | [LinkedIn](#) | [Red Hot Cyber](#)

Recapiti diretti disponibili nella pagina Contatti del sito.



PROFILO

Difendo sistemi, reti e asset critici aziendali guidando la Threat Intelligence e la risposta agli incidenti, e trasformo l'analisi tecnica delle minacce in resilienza operativa e conformità normativa (NIS2, DORA) per il management. Autore e analista CTI per Red Hot Cyber.

ESPERIENZA LAVORATIVA

09/2024 – Attuale

Cyber Security Manager

Digmat S.p.A. · Matera, Italia

- **Team Leadership & Management:** direzione, coordinamento e sviluppo del team di cybersecurity; obiettivi operativi e priorità strategiche.
- **Direzione della Threat Intelligence:** monitoraggio e analisi delle minacce emergenti; tracciamento degli attori malevoli e delle loro TTP.
- **Threat Hunting & Incident Response:** guida delle attività proattive di identificazione delle minacce e coordinamento della risposta agli incidenti.
- **Vulnerability Management:** assessment strutturati e strategie di remediation con i team tecnici.
- **Fonti e decisioni data-driven:** selezione e gestione di fonti OSINT, feed commerciali e network di settore.
- **Strategic Reporting & C-Level Advisory:** reportistica esecutiva per management e stakeholder.
- **Cyber Resilience:** progettazione e ottimizzazione di policy, processi e procedure guidate dall'intelligence.
- **Collaborazione cross-funzionale** con IT, Compliance, Risk Management e Forze dell'Ordine.
- **Security Awareness:** programmi di formazione e sensibilizzazione interna.

09/2022 – 08/2024

SOC Analyst

GPI Cyberdefence S.r.l. · Roma, Italia

- Vulnerability assessment e management; tracciatura e monitoraggio centralizzato degli eventi.
- Analisi sicura di configurazioni di server, data center, sistemi e apparati di rete.
- Digital forensics; analisi statica e dinamica di malware; analisi e report di mail di phishing.
- Gestione degli incidenti con analisi e reportistica; Cyber Threat Intelligence strategica, operativa e tattica.

04/2022 – 09/2022

SOC Analyst (tirocinio curriculare)

GPI S.p.A. · Roma, Italia

Cybersecurity operativa: vulnerability assessment e management, penetration test strutturali e applicativi, monitoraggio centralizzato degli eventi, analisi sicura delle configurazioni e redazione della documentazione tecnica.

03/2021 – 09/2021

IT Supporter

Vestas Italia S.r.l. · Taranto, Italia

Assistenza remota e in sede a clienti e colleghi in ambiente internazionale (lavoro in inglese); manutenzione dell'infrastruttura IT (server room, rete, VoIP, stampanti), gestione delle scorte e della documentazione; test di applicazioni interne e software di sicurezza.

08/2019 – 04/2020

Tirocinio curriculare interno

Università di Bari "Aldo Moro" · Taranto, Italia

Tesi sperimentale sulle tecniche di attacco WPA2 per reti Wi-Fi e studio approfondito dell'architettura.

2013 – 2015	Alternanza scuola-lavoro Wired Soluzioni Informatiche · Taranto, Italia Assistenza hardware e software, assemblaggio e riparazione di PC, installazione di sistemi operativi e driver.
-------------	---

ISTRUZIONE E FORMAZIONE

06/2025 – 03/2026	Corso di perfezionamento «Il professionista della cybersecurity: aspetti regolamentari e operativi» Università degli Studi di Milano Aspetti operativi e normativi della cybersecurity: NIS2, DORA, data governance, analisi del rischio e integrazione con l'intelligenza artificiale.
2020 – 2022	Laurea Magistrale in Sicurezza Informatica (LM-66) – 110 e lode Università degli Studi di Bari "Aldo Moro" Tesi: <i>Digital Forensics: tecniche avanzate di Incident Response mediante utilizzo di tool.</i>
2015 – 2020	Laurea Triennale in Informatica e Comunicazione Digitale (L-31) Università degli Studi di Bari "Aldo Moro" Tesi sperimentale sulle tecniche di attacco WPA2 per reti Wi-Fi.
2010 – 2015	Diploma di Perito Informatico IISS Pacinotti · Taranto, Italia
Obiettivi	CompTIA Security+ (in preparazione) · Master universitario di II livello in Cybersecurity (2027-2028)

CERTIFICAZIONI

07/2024	Cyber Threat Intelligence Professional · Red Hot Cyber
02/2024	Cyber Threat Intelligence 101 · arcX
11/2023 – 11/2028	CSI Linux Certified Investigator (CSIL-CI) · CSI Linux
05/2023	Trend Micro Deep Security 20 for Certified Professionals · Trend Micro
05/2023	Sumo Logic Certified Fundamentals · Sumo Logic
03/2021	Cybersecurity Essentials · Cisco Networking Academy
02/2021	Introduction to Cybersecurity · Cisco Networking Academy
02/2021	Networking Essentials · Cisco Networking Academy
02/2021	Elements of AI · Reaktor · Università di Helsinki

Le certificazioni sono verificabili online dalla pagina [Certificazioni del sito](#).

COMPETENZE

Intelligence	Cyber Threat Intelligence, OSINT / HUMINT, Traffic Light Protocol, Dark Web, monitoraggio data leak site e gang ransomware
Blue Team & DFIR	Incident Response, Digital Forensics, analisi statica e dinamica di malware, Threat Hunting, Event Analysis
Strumenti	Sumo Logic SIEM, Trend Micro Deep Security, CSI Linux, MySQL
Governance & GRC	Direttiva NIS2, Regolamento DORA, data governance, analisi del rischio, AI
Trasversali	Leadership, problem solving, pianificazione e organizzazione, lavoro individuale e in team

LINGUE

Italiano: madrelingua · **Inglese:** C1 (ascolto, lettura, scrittura, produzione e interazione orale)