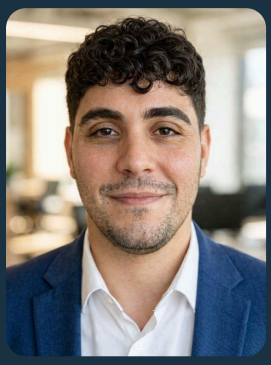
joele bernardi

Junior Cybersecurity Analyst | SOC & Incident Response



joelebernardi0@gmail.com

3520685267

Aprilia, latina

linkedin.com/in/joele-bernardi-865561405

italiano

14/11/2001

SUMMARY

Junior Cybersecurity Analyst con solide basi in sicurezza informatica, analisi dei log, gestione degli alert e principi di incident response. Esperienza pratica su Windows, Linux, networking e strumenti di sicurezza maturata tramite laboratori EPICODE e piattaforme come TryHackMe. Approccio analitico, capacità di problem solving e forte motivazione a crescere in contesti IT e cybersecurity, sia operativi che di supporto tecnico.

LANGUAGES

Inglese

Italiano

spagnolo

EDUCATION

EPICODE | Cybersecurity - ethical hacker

03/2026 – 06/2026

Percorso intensivo di oltre 450 ore live focalizzato su sicurezza informatica, ethical hacking e difesa cyber. Il programma include:

- **Fondamenti di sicurezza informatica**: hacking etico, threat landscape, costruzione di un lab virtuale
- **Networking & protocolli**: TCP/IP, DNS, HTTP/HTTPS, firewall, VPN
- **Sistemi operativi**: Windows, Linux, Kali, gestione utenti, permessi, servizi di rete
- **Python per la cybersecurity**: scripting, automazione, analisi dati di sicurezza
- **Penetration Testing & Attacco/Difesa**:
- Raccolta informazioni
- Scansione e enumerazione
- Exploit e vulnerabilità
- Social engineering
- Attacchi a reti, sistemi e web app
- Uso avanzato di Metasploit
- Simulazioni su ambienti reali e dark web
- **Malware Analysis (base)**: riconoscimento malware, analisi comportamentale, static analysis
- **SOC & Incident Response**: monitoraggio eventi, analisi alert, risposta agli incidenti, uso di Splunk
- **OSINT & Threat Intelligence**: raccolta informazioni, analisi indicatori, strumenti TI
- **AI & Cybersecurity**: prompt design, GitHub Copilot, uso dell'AI per mappare vulnerabilità e difese
- **Build Week**: progetti pratici di gruppo per simulare un contesto lavorativo reale

SKILLS

Competenze Tecniche

- Analisi dei log (Windows Event Logs, Syslog)
- Gestione e monitoraggio degli alert
- Principi di Incident Response
- Sistemi operativi: Windows, Linux
- Networking: TCP/IP, DNS, HTTP/HTTPS, VPN
- PowerShell e CMD (basi)
- OSINT & Threat Intelligence (VirusTotal, OTX, AbuseIPDB)
- Sicurezza endpoint (EDR – basi)
- Analisi statica malware (PE-bear, CFF Explorer)

Competenze Trasversali

- Problem solving
- Attenzione ai dettagli
- Capacità analitiche
- Lavoro in team
- Gestione dello stress
- Comunicazione chiara e professionale