Marco Fornari

Junior SOC Analyst | Developer

CONTATTI

25/01/1997 +39 3890279515 Patente B

marco.fornari.97@gmail.com

Via Augusto Murri 20, Fermo (FM)

Linkedin Github

PRESENTAZIONE

Profilo junior orientato a security operations e system engineering, con esperienza pratica in detection di minacce email, analisi di log e Threat Intelligence su ambienti Linux containerizzati.

Ho progettato una piattaforma anti-phishing e Business Email Compromise per PMI: analisi di header e URL per l'estrazione degli IoC, correlazione su 5 feed di Threat Intelligence e risk scoring a supporto del triage e dell'escalation degli eventi, con rate limiting, caching e fallback per la continuità del servizio.

Formazione in Cybersecurity, Cyber Risk e Data Protection (Università Politecnica delle Marche, Google Cybersecurity Certificate). Diploma ITS in Industrial Software Development, 110/110 e lode. CEH in preparazione.

PROGETTI

Portfolio personale security-first (Astro/Netlify): architettura statica per minimizzare la superficie d'attacco, hardening HTTP completo validato A+ su securityheaders.com (CSP, HSTS, X-Frame-Options, Permissions-Policy), SAST con Semgrep e ruleset custom con triage dei finding, SCA delle dipendenze con npm audit e supporto alla vulnerability remediation. → mfornaridev.netlify.app

ESPERIENZE LAVORATIVE

JUNIOR DEVELOPER — SECURITY ENGINEERING

02/2026 – 07/2026

Overside srl - Porto San Giorgio (FM)

Sviluppo di Overguard, piattaforma di email security anti-phishing e Business Email Compromise per PMI.

· Detection di phishing e BEC tramite analisi automatizzata di header SMTP, mittente, dominio e URL, con estrazione e correlazione degli IoC.
· Risk scoring multi-segnale su 5 feed di Threat Intelligence (VirusTotal, Google Safe Browsing, URLScan.io, Hybrid Analysis, AlienVault OTX) a supporto del triage e dell'escalation degli eventi.
· Continuità del servizio di detection con rate limiting per provider, caching dei verdetti e fallback tra le fonti; modulo DLP semantico sui contenuti in uscita.
· Backend .NET 10 in Clean Architecture, PostgreSQL, API REST con autenticazione JWT, deployment Docker su Linux; estensioni Chrome MV3 e Thunderbird MV2 integrate con il backend.

Stack: Linux · Docker · PostgreSQL · REST API · JWT · .NET 10 · Threat Intelligence · IoC · DLP

JUNIOR DEVELOPER

04/2025 – 01/2026

Levante Yachts srl - Porto San Giorgio (FM)

Automazione della pubblicazione dei contenuti del portale via API REST (WordPress, Google Sheets); gestione del database MySQL con query SQL per verifica e bonifica dei dati; sviluppo frontend/backend (HTML, CSS, JavaScript, PHP).

VIDEOMAKER E FOTOGRAFO 01/2022 – 09/2024

Freelancer - Colleferro (RM)

Gestione autonoma del ciclo completo di progetto: raccolta requisiti con il cliente, pianificazione, esecuzione tecnica e consegna nei tempi concordati, con interfaccia diretta con il referente cliente.

FORMAZIONE

DIPLOMA ISTITUTO TECNICO SUPERIORE - ITS SMART ACADEMY 28/10/2024 – 19/06/2026

Votazione: 110 e lode

ITT MONTANI DI FERMO (FM)

Livello 5 EQF

CORSO DI PERFEZIONAMENTO IN CYBERSECURITY, CYBER RISK AND DATA PROTECTION 12/04/2024 – 13/09/2024

Università Politecnica delle Marche - Ancona (AN)

Formazione in Cybersecurity e Data Protection con focus su GDPR, cyber risk e gestione della sicurezza. Argomenti:

- protezione di dati e reti; sicurezza di software e sistemi informatici;
- valutazione e mitigazione del rischio;
- normativa e privacy;
- aspetti legali ed etici della gestione delle informazioni.

25 CFU · Tesi: “Strategie avanzate di gestione del rischio”

Laurea Triennale in Arti e Scienze dello Spettacolo 09/2017 – 01/2021

Sapienza Università di Roma - Roma (RM)

Liceo delle Scienze Applicate 2011 – 2016

ITIS Cannizzaro - Colleferro (RM)

CERTIFICAZIONI

2026 - In corso

CEH (Certified Ethical Hacker) — Preparazione in corso

Preparazione teorico-pratica su ethical hacking, vulnerabilità, sicurezza di reti e sistemi.

Cybersecurity Certificate Google - Coursera

02/2024 - 06/2024

- Completato otto corsi sviluppati da Google con valutazioni pratiche.
- Competenze in Python, Linux, SQL, strumenti SIEM (Security Information and Event Management) e sistemi IDS (Intrusion Detection Systems).
- Capacità di identificare rischi, minacce e vulnerabilità comuni nella cybersecurity e tecniche di mitigazione.

Certificate in English — Cambridge English B2

2023

Inlingua Frosinone - Frosinone (FR)

COMPETENZE DIGITALI

Hard Skill

Sistemi e container: Linux (processi, networking, analisi log), Docker, ambienti on-prem e containerizzati
Security operations: analisi header/URL email, correlazione IoC, risk scoring, triage ed escalation, DLP
Threat Intelligence: VirusTotal · AlienVault OTX · URLScan.io · Hybrid Analysis · Google Safe Browsing
Application security: hardening HTTP (CSP, HSTS), SAST/SCA con Semgrep e npm audit, triage dei finding
Database e troubleshooting: SQL, PostgreSQL, MySQL, Entity Framework, debug API REST, analisi log
Scripting e sviluppo: Bash · C#/.NET · JavaScript · PHP · Python · Git · JWT · REST API
Fondamenti da percorsi formativi: SIEM, IDS, Risk Assessment, GDPR
Lingue: Italiano (madrelingua) · Inglese B2

Soft Skill

Pensiero analitico e critico · Problem solving · Attenzione al dettaglio · Documentazione e reportistica tecnica · Collaborazione · Gestione autonoma dei progetti