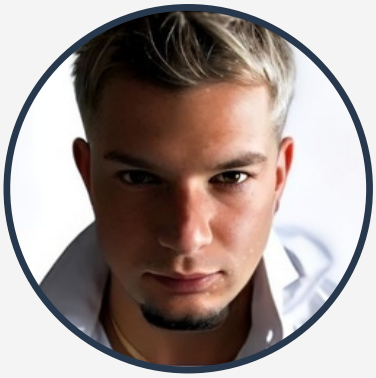
LORENZO GAROFFOLO

IT Security Specialist | Red Team Enthusiast

Telefono
+39 366 199 5209

Email
lorenzo.garoffolo03@gmail.com

Indirizzo
(PD) Piove di Sacco



About Me

La mia formazione in informatica e il percorso di specializzazione in Cybersecurity hanno rafforzato una passione concreta per la sicurezza informatica, lo sviluppo e la gestione di ambienti digitali moderni.
Mi interessa contribuire alla creazione e al mantenimento di sistemi innovativi, aggiornati e sicuri, capaci di unire efficienza, affidabilità e protezione.
Mi ritengo una persona curiosa, proattiva e orientata alla sperimentazione, con il desiderio costante di approfondire nuove tecnologie e trasformarle in soluzioni utili, solide e ben strutturate

Skills

Hard

- Microsoft 365 Administration
- Entra ID / Active Directory
- Open Source Intelligence (OSINT)
- Incident Response
- Microsoft Sentinel
- Security Operations
- SIEM / EDR
- Threat Hunting
- Log Analysis
- Identity & Access Management
- Exchange Online / SharePoint
- Endpoint Management
- Phishing Analysis
- Asset Management
- Remote Support
- LLM Integration
- Workflow Automation
- AI Application Development

Soft

- Leadership
- Analytical Problem Solving
- Cross-team Collaboration
- Adaptability
- Time Management
- Priority Management
- Attention to Detail
- Stakeholder Communication
- Decision-Making Under Pressure

Education

Informatica, Diploma Perito Informatico — 2017 - 2022
ITI Cardano (A. EINSTEIN), Piove di Sacco

- programmazione: java, c++
- sviluppo web: css, html, js

CyberSecurity, ITS corso biennale specialistico — 2023 - 2025
Digital Academy “Mario Volpato”

- programmazione: Python
- Social engineering
- SAST
- Pentesting
- Reti e comunicazione
- Criptografia

Experience

Cybersecurity Analist — 2023
Carel, Brugine(PD)

- Studio di normative di sicurezza: Approfondimento delle normative GDPR, ISO/IEC 27001 e, più recentemente, della Direttiva NIS2, per garantire la conformità aziendale alle leggi e agli standard di sicurezza.
- Gap Analysis: Identificazione delle lacune tra le policy aziendali esistenti e gli standard di sicurezza previsti dalle normative, proponendo miglioramenti e strategie di adeguamento.
- Analisi dei log: Utilizzo di Splunk per l'analisi approfondita dei log al fine di rilevare anomalie, potenziali minacce e attività sospette, migliorando il livello di sicurezza aziendale.
- Attività di OSINT: Condotte analisi di intelligence open-source per identificare potenziali minacce esterne che potrebbero compromettere la sicurezza dell'organizzazione.

Cybersecurity Specialist — 2024
SimplyIT, Padova

- Implementazione di un SIEM Wazuh in ambiente virtuale, con configurazione delle regole e integrazione di servizi esterni come VirusTotal per migliorare la visibilità e la gestione della sicurezza.
- Utilizzo della console Cynet per l'analisi di log e alert, al fine di identificare e risolvere potenziali vulnerabilità e minacce.
- Progettazione e sviluppo di soluzioni interne, tra cui studi su bypass di Defender, simulazioni di attacchi (Red Teaming) e software per l'estrazione di informazioni aziendali tramite OSINT e fonti closed.
- Integrazione di un database di leak per monitorare e confrontare i dati aziendali e ricevere alert tempestivi in caso di breach, permettendo la pronta comunicazione ai clienti per mitigare i rischi di sicurezza.

Passion

Sono appassionato di sviluppo web, automazione e tecnologie digitali e, nel tempo libero, mi dedico alla progettazione e realizzazione di siti e applicazioni web, lavorando sia sul backend che sul frontend con framework come Django e Laravel. Questa attività mi permette di affinare continuamente le mie competenze tecniche, sperimentare nuove architetture e sviluppare soluzioni scalabili, sicure e performanti. Negli ultimi tempi ho esteso il mio interesse anche ai sistemi di intelligenza artificiale, approfondendo i modelli linguistici (LLM) e integrandoli nei miei progetti per costruire applicazioni più dinamiche, automatizzate e capaci di offrire interazioni evolute. Attraverso questi progetti coltivo un approccio pratico, curioso e orientato all'innovazione, con particolare attenzione alla qualità del codice, all'affidabilità dei sistemi e al valore concreto delle soluzioni sviluppate.

IT security Analist — 2025

Unox, Cadoneghe (PD)

- Gestione operativa di infrastrutture ed ecosistemi Microsoft aziendali, con attività quotidiane su Microsoft 365, Entra ID, Exchange Online, SharePoint, Active Directory e amministrazione degli account utente, contribuendo alla continuità operativa, alla sicurezza degli accessi e al corretto funzionamento dei servizi digitali.
- Gestione di incidenti e anomalie legate a identità digitali e sicurezza degli accessi, con attività di reset password, blocco e sblocco utenze, revoca di sessioni attive, contenimento di account compromessi, verifica di accessi sospetti e supporto operativo alle attività di remediation
- Monitoraggio e analisi di eventi di sicurezza tramite Microsoft Sentinel e strumenti di supporto, con attività di triage degli alert, gestione di falsi positivi, investigazione di eventi anomali, analisi tramite shell e coordinamento operativo con SOC esterno e team tecnici per la gestione e risoluzione degli incidenti
- Gestione di campagne phishing e segnalazioni di sicurezza, con identificazione delle minacce, smantellamento dei casi, supporto al contenimento, comunicazione agli utenti coinvolti e collaborazione con i referenti tecnici per il ripristino delle condizioni di sicurezza
- Supporto tecnico e operativo su endpoint, postazioni di lavoro e dispositivi aziendali, inclusa configurazione iniziale, manutenzione, assistenza remota, assegnazione asset, attivazione SIM, gestione del ciclo di vita dei dispositivi e risoluzione di problematiche hardware/software in contesto enterprise
- Gestione ticket IT e security, supporto utenti, coordinamento con team interni ed esterni e operatività in contesti ad alta continuità di servizio, maturando autonomia, problem solving, rapidità decisionale e capacità di gestione sotto pressione anche in regime di reperibilità

Personal Projects

SickFitPro

Piattaforma fitness intelligente basata su AI progettata per automatizzare il monitoraggio nutrizionale, la pianificazione degli allenamenti e l'analisi dei progressi attraverso modelli linguistici e computer vision

- AI Assistant contestuale con memoria utente.
- Riconoscimento alimentare tramite AI Vision
- Stima automatica di calorie e macronutrienti da immagini.
- Sistema di raccomandazione basato su storico, obiettivi e comportamento dell'utente
- Architettura cloud-native con sincronizzazione realtime.
- Implementazione di controlli security e gestione sicura dei dati

Planica

Progettazione e sviluppo di una piattaforma intelligente che combina task management, calendar planning, knowledge management e Intelligenza Artificiale in un unico ecosistema operativo personale

- Assistente AI con memoria contestuale
- Generazione automatica di task e pianificazioni
- Sistema di fallback multi-LLM per garantire continuità operativa
- Gestione centralizzata di conoscenza, documenti e idee
- Dashboard produttività e monitoraggio obiettivi
- Automazione dei workflow personali e professionali