

GIORGIO LOGGIA

xmreur@gmail.com

+39 351 606 4122

Milano, Lombardia, Italia

github.com/xmreur

ABOUT ME

Passionate about computers since early childhood.
I started programming at 11, driven by a love for video games, which fostered a strong technical foundation and a continuous appetite for learning. My journey later focused on cybersecurity, initially exploring offensive security, including vulnerability research and discovery of zero-day exploits in major companies. I then transitioned to ethical hacking as a white hat, specializing in Blue Team activities, with a focus on threat defense, prevention, and mitigation.

EDUCATION

ITIS G. Feltrinelli
2022-Current
Milano, Italy

LANGUAGES

Italian (Native)
English (Second language - C1)

WORK EXPERIENCE

Cybersecurity audit | Mondovela

Jun 2023 - Nov 2025

*Performed **comprehensive cybersecurity audits**, identifying **potential data breaches** and vulnerabilities, updating **compromised credentials**, and implementing a **company-wide password manager** to enhance **information security** and reduce the risk of **unauthorized access**. Additionally, redesigned the **internal file-sharing infrastructure** by migrating from a traditional **NAS** system to a **Google Drive-based** solution, enabling **secure external access** with **email-based** access controls, improving collaboration efficiency, and strengthening overall organizational security protocols.*

B-Connekt - Developer | Biteck S.R.L.

Sept 2024 - Jan 2025

***Designed and developed B-Connekt**, an internal platform for centralizing **client data, contacts, and scheduling**, featuring **role-based access control**, a contact book, a **Google Calendar-style event system**, a **clean web UI**, and **secure APIs**. Built as a **Flask-based CMS**, the platform supports **real-time** collaboration, **granular permissions**, and **CSV import/export** for seamless **data portability**, enhancing team efficiency and client management. Key contributions included **system design, database architecture, real-time functionality**, and implementation of **role-based access control** to ensure secure and flexible access management.*

Co-Founder | UnicodeIt

Dec 2022 - Feb 2023

***Co-founded UnicodeIt**, a **web development** startup serving **small and medium-sized businesses** as well as **private clients**, in collaboration with schoolmate Alessandro Mannarà. Contributed to **team collaboration, website design, web development**, and **entrepreneurship**, establishing the foundation for the company's operations and client projects.*

SKILL MATRIX

Category	Key Skills	Proficiency
Programming	TS/JS, Go, Python, Java, Kotlin, Rust, C, C++, C#, Bash	Strong: TS/JS, Go, Python, Java
Cybersecurity	Pen Testing, Ethical Hacking, Tor, Zero-Days	Hands-on ethical/privacy
Database	Sqlite, PostgreSQL, MongoDB, Redis, Firebase	SQL/NoSQL
DevOps	Linux, GitHub, P2P, Multi-OS	System-level comfort

PROJECTS & TOOLS DEVELOPED

Cyra - XDR Platform

*Cyra is a complete, open-source **Extended Detection and Response (XDR) platform** featuring both a lightweight Python agent for Windows endpoints and a web UI dashboard for centralized management. The agent monitors processes, network traffic, and filesystem in real-time using YAML rules, while the **SIEM-like web UI** displays alerts, tracks online agents, and enables threat response across deployments.*

Key Features:

- Agent telemetry for filesystem, process, and network events with YAML detection rules (blacklists, severity scoring, thresholds)
- Windows-specific response: TCP/UDP blocking via ctypes API, process kill/suspend, memory snapshots on alerts
- Web UI dashboard showing real-time alerts, agent status (online/offline), and agent inventory management
- Centralized SIEM capabilities: rule visualization, event filtering, historical logs, and cross-agent correlation
- Modular architecture allowing agent-to-server event forwarding for scalable endpoint fleets

Technologies Used:

- **Python** - Agent core with psutil, ctypes for Windows APIs, and YAML for dynamic rules
  NextJS - >Web UI Dashboard for alerts and agent management
- **psutil & ctypes** - Endpoint monitoring and low-level network/process control
- Event forwarding protocol between agents and central server for real-time UI updates
- Platform focus on Windows with extensible backends for Linux/macOS

Prysm - https://prysmchat.xyz

*In response to the European Union's proposed **Chat Control** legislation, which introduced significant **mass-surveillance** concerns, I developed **Prysm**, a **privacy-centric, cross-platform P2P messaging prototype** built with **Flutter**. The system is architected to **operate natively over Tor**, utilizing **onion routing** to provide **censorship- and surveillance-resistant communication**.*

Security-Focused Features:

- End-to-end encryption with messages secured on-device and decrypted only at the peer.
- Tor onion routing with multiple relay hops for untraceable communication patterns
- No-server architecture using cryptographic keys for identities, preventing faulty central points
- Cross-platform UI with anonymous transport, designed for journalists, activists, and privacy enthusiasts
- Distributed P2P model resistant to blocking, with battle-tested protocols for maximum security

Technologies Used:

- **Flutter** - Core Cross-Platform development for mobile and desktop UI
- **TOR (JNI/Embedded)** - Onion routing and SOCKS proxy for P2P transport
- **RSA 4096 & AES256** - Cryptography for key exchange and message encryption
- **bs58 & Flyer Chat** - Identity encoding and chat interface components
- **Platform channels** - Native integration for Tor daemon control and networking

Fluxa - Issue Tracker

*Fluxa is a lightweight, open-source **issue, bug, and feature proposal tracker** built with React and Supabase. The platform enables teams to manage projects **efficiently** with **real-time updates**, focusing on clarity and speed for tracking active tasks, completions, and assignments **without complex workflows**.*

Key Features:

- Teams and role-based access (owner, admin, member) with users belonging to multiple teams.
- Project organization under teams with project-level permissions
- Issue lifecycle management (bugs, features, proposals) with assignment, priority, and timestamps
- Comments for collaboration, customizable labels for filtering, and voting on proposals
- Realtime capabilities powered by Supabase for instant updates across users

Technologies Used:

- **React** - Modern frontend framework for responsive UI
- **Supabase** - Backend for authentication, realtime database, and storage
- Role-based permissions and team/project hierarchy via Supabase auth and PostgreSQL
- Simple, intuitive workflows emphasizing speed and minimalism

SeedPass - Seed-Based Password Deriver

*SeedPass is a privacy-focused, web-based **password deriver** that generates site-specific credentials from a master seed vault. Users unlock with a seed phrase, input domain/app/username/length, and derive **deterministic, reproducible passwords** with no storage, full client-side for ultimate security and portability.*

Key Features:

- Master seed vault unlock to access derivation engine
- Per-site derivation: Enter domain (es. example.com), app name, username/email, custom length (es. 16 chars)
- One-click "Derive" generates unique, strong password - regenerate identically anywhere with same seed/inputs
- Dark-themed, responsive UI with lock/unlock vault toggle
- Zero server storage: All logic client-side for privacy-first password management

Technologies Used:

- **Next.js / React** - Modern frontend for responsive, interactive password vault UI
- **Vercel** - Zero-config deployment, edge caching, and preview features
- Client-side seed derivation logic (**BIP-85 style**) for secure, stateless password management

www.cybersentinels.net
2024 - Present

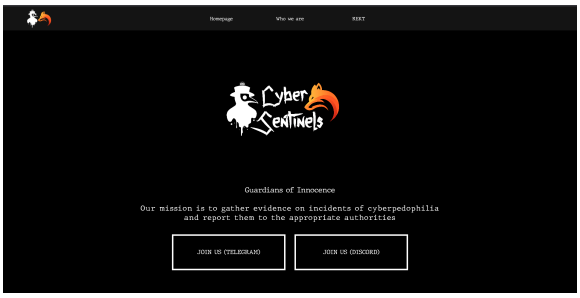
***Cyber Sentinels** is a **volunteer-driven cybersecurity initiative** with over **1,500 active members**, focused on the **identification, documentation, and reporting of online child exploitation activities** as well as **cybersecurity training**. Joined in its early days as a **regular member**, quickly demonstrating **technical expertise** and **leadership skills**, and advanced to **Owner & Technical Lead** within the first year.*
***Designed and developed the organization's full-stack website** and created numerous **internal tools** used by the team to streamline operations, track threats, and manage cybersecurity initiatives.*
***Collaborated closely with founders Volpe and Dottore** to **coordinate operations** and **manage strategic initiatives**, contributing to the organization's mission of **safeguarding children online** and enhancing the effectiveness of the team's **technical operations**.*

Key Responsibilities & Achievements

- **Developed internal tools for secure evidence collection,** handled community
- Coordinated with international law enforcement bodies to facilitate the submission of actionable intelligence and case data.
- Advocated for digital safety and child protection through public awareness campaigns and social media outreach.
- Livestreamed some operations on TikTok to spread awareness in more people.
- CyberSentinels was then featured in **Vanity Fair (2025) for outstanding work in digital child protection and grassroots cyber activism**

Skills Applied:

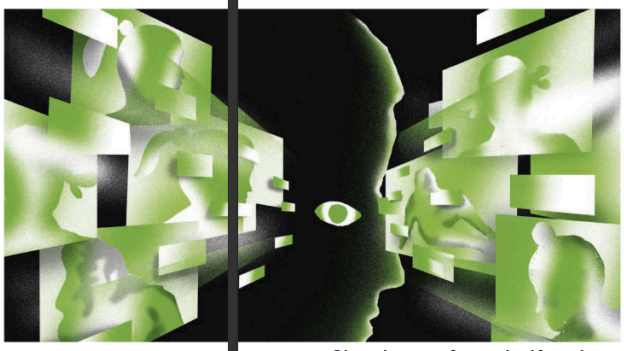
- Cyber Thread intelligence
- Digital forencics
- OSINT (Open Source Intelligence)
- SEO (Search Engine Optimization)
- Incident reporting and triage
- Community building and leadership
- Ethics in cybersecurity
- Cybersecurity education and training



I GUARDIANI *dei bambini*

Hanno tra i 20 e i 30 anni, sono esperti di cyber security e passano il loro tempo online a catturare i pedofili. Abbiamo incontrato su Telegram gli HACKER ETICI: ci hanno raccontato gli orrori del dark web con gli orchi che fanno tutti la stessa domanda: «Sei in pigiama?»

di **VERONICA BIANCHINI** *illustrazione* **DANIEL ZENDER**



«Ciao Cate13, ho 50 anni, è un problema per te?». Comincia così, di solito, la conversazione online tra un pedofilo e la sua vittima minorenne. Ce lo spiegano due *hacker* che hanno fatto della caccia a questi criminali la loro missione. Incontro Volpe e Dottore su Telegram. Tutte le nostre conversazioni si svolgeranno su questa piattaforma, che è anche il luogo dove incastrano i criminali. La loro identità resterà ignota. Esperto di *cyber security* sui trent'anni il primo e studente ventenne il secondo, hanno fondato il gruppo Cyber Sentinels, che oggi conta oltre mille persone. Nascondere i loro nomi e il loro volto è una precauzione per poter continuare a cacciare. Sono *white hat hacker*, ovvero superesperti di web e sistemi informatici, che usano le loro competenze in modo etico per difendere le aziende, aiutare la comunità e identificare e denunciare chi cerca di adescare ragazzini online. Tutto è nato a ottobre quando, raccontano, «abbiamo deciso di fondare il nostro movimento con due scopi principali: da un lato l'attivismo, con l'impegno di scovare i pedofili e denunciarli alle autorità; dall'altro la formazione gratuita per chi vuole avvicinarsi alla sicurezza informatica e all'*hacking* etico. In molti si sono uniti. Ci sono esperti di diversi settori: avvocati, ingegneri, studenti, curiosi e poi qualche decina di cacciatori». In pochi mesi hanno già incastrato quasi duecento tra i peggiori criminali, quelli che non si fanno scrupolo di avvicinare ragazzini e ragazzine e poi farsi mandare foto, video e se possibile incontrarli nella vita reale. «Noi *hunter*», spiega Volpe, «siamo organizzati gerarchicamente. In base alle competenze e al numero di prede cacciate, si va da una a tre stelle. Poi c'è Gorosei, che è la responsabile di tutto il gruppo e verifica, per esempio, che i cacciatori siano maggiorenni». La ricerca dei pedofili comincia sulle chat pubbliche, alle quali si può accedere anonimamente, con un semplice *nickname*, e dove si può dialogare liberamente con gli altri utenti. «Entriamo in canali come Amicizia, Chat Italy e così via e fingiamo di essere bambine», racconta Volpe. «Quando mi iscrivo con un *nickname* femminile, ricevo tantissimi messaggi privati. A chi mi contatta, dico: "Ciao, piacere, Sara, 13 anni, Roma". Alcuni rispondono: "Troppo piccola". Altri vanno avanti: quelli sono il nostro obiettivo. Molti dichiarano subito la loro vera età, solo alcuni si fingono ragazzini. Nel novanta per cento dei casi, come prima cosa chiedono: "Sei in pigiama?". E io capisco che non ci resta che "cucinarli"».

Cucinare, in questo contesto, significa: agganciarli, incastrarli, identificarli e consegnarli alle autorità. Il copione è sempre lo stesso, di solito infallibile. I cacciatori si fingono una ragazzina con una storia difficile alle spalle. Grazie a tecniche di ingegneria sociale, e una sottile manipolazione, spingono il pedofilo a scoprirsi. Racconta Dottore: «Dico che mio padre è morto. Questi individui, invece di dimostrare un minimo di empatia, diventano più spavaldi poiché pensano che l'assenza di una figura genitoriale mi renda una preda più vulnerabile. Scambiamo qualche messaggio sulla chat pubblica, poi con una scusa li porto su Telegram, e il gioco è fatto».

«Dico che sono Sara e ho 13 anni. Alcuni rispondono: "Troppo piccola". Altri vanno avanti e li incastriamo»

Sulla piattaforma di messaggistica istantanea gli *hacker* hanno più spazio di manovra e riescono a risalire più facilmente all'identità dei pedofili. «Usiamo diversi *tool*, grazie ai quali possiamo scoprire chi sono», spiega Dottore. A differenza di quello che normalmente si pensa, dopo l'arresto del fondatore Pavel Durov, Telegram ha cambiato le proprie policy e ha dato la possibilità alle autorità di risalire al numero di telefono e all'indirizzo IP degli utenti. I pedofili, però, la usano senza farsi tante domande: «Sembrano quasi ipnotizzati dal fatto che dall'altra parte ci sia una ragazzina. Appena inizia la conversazione, ci chiedono di inviare foto o video delle parti intime. Oppure, siamo noi a offrirci di mandarli e loro acconsentono. Nel momento in cui rispondono di sì, già si configura un reato, poiché sarebbero immagini pedopornografiche. Il passo successivo è combinare un incontro. Di solito diciamo: "Ci vediamo, vieni a trovarmi? Mamma esce e ho casa libera". Immancabilmente accettano. L'ultimo passo è ottenere una loro foto. Una volta raccolti questi elementi, non rispondiamo più ai loro messaggi». A quel punto scattano le verifiche sull'identità: bisogna capire chi c'è dall'altra parte, essere sicuri che sia maggiorenne e che la foto inviata corrisponda al vero. Qui entra in gioco la bravura degli *hacker*. Ma chi sono i pedofili? C'è un profilo tipico? «Nella nostra esperienza sono tutti uomini», dice Volpe, «il più giovane aveva meno di trent'anni, il più vecchio una settantina. Provenienti da ogni parte d'Italia. Abbiamo incontrato anche ingegneri o persone che si esprimevano con proprietà di linguaggio, ma la maggior parte non sembra molto istruita». Una volta smascherati i criminali, il passaggio finale è quello di preparare una cartella digitale con tutta la documentazione raccolta: foto, chat, nome, numero di telefono, indirizzo email, profili social. Tutte queste informazioni vengono caricate sul portale del Moige, il Movimento italiano genitori, oppure, più spesso, su quello del Telefono Azzurro. Il fascicolo viene poi inviato alla polizia postale, che si attiva immediatamente. «La cyberpedofilia è forse il crimine informatico più grave che esista», precisa Volpe. «Nei forum del *dark web*, anche dove si vendono droga, *malware* o servizi di frodi, è sempre vietato il materiale pedopornografico. Infatti, è risaputo che quando arriva una denuncia per cyberpedofilia o pedopornografia, le forze dell'ordine si mobilitano subito».

Ma cosa si può fare per cercare di tutelare i bambini e i ragazzi ed evitare che corrano rischi? «Il mio consiglio è dare loro il cellulare il più tardi possibile», dice Dottore, «è importante creare account con limitazioni, contingentare l'uso del telefono e installare software di *parental control*, ma anche monitorare proattivamente l'attività in Rete dei ragazzi, facendo sempre attenzione ai siti e alle app che usano e con chi entrano in contatto. Anche sui videogiochi si possono fare brutti incontri, bisogna spiegarlo ai più giovani e tenere costantemente gli occhi aperti, perché internet può essere un posto pericoloso».

➡ TEMPO DI LETTURA: **7 MINUTI**