Lorenzo Bianchi | Ingegnere della cybersicurezza

Via Torino 45, Milano, Lombardia, Italia, 20123
+39 02 8765 4321 • lorenzo.bianchi@lorenzobianchi.it • https://www.lorenzobianchi.it
@lorenzo-bianchi-cyber • @lorenzobianchi

Informazioni personali

Professionista della sicurezza informatica con oltre otto anni di esperienza nella protezione di infrastrutture critiche e dati sensibili. Specializzato in monitoraggio, risposta agli incidenti e architetture Zero Trust, unisco competenze tecniche e visione del rischio per sostenere gli obiettivi aziendali.

- Guido progetti di adeguamento a NIS2, GDPR e ISO 27001.
- Coordino team di analisti e collaboro con sviluppo, reparti operativi e ufficio legale.
- Progetto controlli preventivi e promuovo una cultura della sicurezza misurabile.

Formazione

Politecnico di Milano **https://www.polimi.it**
Laurea magistrale, Ingegneria Informatica, Punteggio: 110/110 con lode *set 2014–lug 2016*

- Tesi magistrale sulla rilevazione di intrusioni in ambienti cloud tramite tecniche di apprendimento automatico.
- Approfondimento su crittografia applicata, sicurezza delle reti e gestione del rischio.
- Partecipazione a laboratori di hacking etico e progetti con aziende del territorio.

Corsi: Sicurezza dei sistemi informativi, Crittografia applicata, Architetture di rete e protocolli, Sistemi operativi e virtualizzazione, Gestione dei rischi informatici, Diritto delle nuove tecnologie

Università degli Studi di Bologna **https://www.unibo.it**
Laurea triennale, Ingegneria Informatica, Punteggio: 108/110 *set 2011–lug 2014*

- Basi solide di programmazione, algoritmi, reti e basi di dati.
- Progetto finale su un sistema di autenticazione a due fattori per applicazioni web.
- Esperienza in gruppi di lavoro e presentazioni tecniche.

Corsi: Fondamenti di programmazione, Algoritmi e strutture dati, Reti di calcolatori, Basi di dati, Sistemi operativi

Esperienza professionale

Finanza Sicura S.p.A. **https://www.finanzasicura.it**
Ingegnere della cybersicurezza senior *mar 2020–Presente*

- Guido un gruppo di sei analisti nella gestione di incidenti di sicurezza su scala nazionale.
- Ho progettato e implementato un modello di difesa Zero Trust per 4.000 dipendenti e 120 applicazioni.
- Ho ridotto del 35% il tempo medio di rilevamento e contenimento delle minacce tramite regole SIEM e automazione SOAR.
- Coordino verifiche ISO 27001 e attività di adeguamento alla direttiva NIS2.
- Collaboro con i team di sviluppo per integrare controlli di sicurezza nella catena CI/CD.

Parole chiave: Gestione del rischio, SIEM, Zero Trust, Conformità, Risposta agli incidenti

CloudNova S.r.l. **https://www.cloudnova.it**
Cybersecurity Analyst *set 2016–feb 2020*

- Monitoraggio continuo di eventi di sicurezza con SIEM, IDS/IPS e piattaforme EDR.
- Analisi di malware, phishing e tentativi di accesso anomalo, con redazione di rapporti tecnici.
- Gestione delle vulnerabilità e coordinamento delle correzioni con i gruppi infrastrutturali.
- Supporto nella definizione delle politiche di accesso e nella formazione del personale.

Parole chiave: Monitoraggio, Analisi delle minacce, Firewall, VPN, Vulnerabilità

TecnoReti S.p.A. **https://www.tecnoreti.it**
Specialista di rete junior *ott 2014–ago 2016*

- Configurazione e manutenzione di apparati di rete, firewall e VPN tra sedi.
- Diagnosi e risoluzione di problemi di connettività e sicurezza per sedi distribuite.
- Collaborazione alla migrazione verso un'infrastruttura di rete segmentata.

Parole chiave: Networking, Troubleshooting, Cisco, Segmentazione

Lingue

Italiano: Madrelingua o bilingue — **Parole chiave**: Madrelingua

Inglese: Competenza professionale completa — **Parole chiave**: IELTS 7.5, Livello C1

Francese: Competenza professionale limitata — **Parole chiave**: DELF B1

Competenze

Sicurezza informatica: Esperto — **Parole chiave**: SIEM, IDS/IPS, Penetration testing, Threat hunting, Risposta agli incidenti

Sicurezza cloud: Avanzato — **Parole chiave**: AWS, Azure, Kubernetes, IAM, Terraform

Governance e conformità: Avanzato — **Parole chiave**: ISO 27001, NIS2, GDPR, Valutazione del rischio, Verifiche di conformità

Programmazione e automazione: Avanzato — **Parole chiave**: Python, Bash, PowerShell, SQL

Premi

Premio Innovazione in Cybersecurity

Associazione Italiana per la Sicurezza Informatica — *nov 2022*

Riconoscimento per il progetto di una piattaforma di condivisione di indicatori di compromissione tra piccole e medie imprese italiane, con impatto misurabile sulla riduzione degli incidenti.

Certificazioni

Certified Information Systems Security Professional (CISSP) — **https://www.isc2.org/certifications/cissp**

ISC2 — *giu 2021*

AWS Certified Security - Specialty — **https://aws.amazon.com/certification/certified-security-specialty/**

Amazon Web Services — *ott 2022*

ISO/IEC 27001 Lead Auditor — **https://www.tuv.com/italy/it/**

TÜV Italia — *apr 2023*

Pubblicazioni

Rivista Italiana di Cybersecurity — **https://www.rivistaitalianacybersecurity.it/articoli/supply-chain**

Difendere la supply chain software: modelli e pratiche — *set 2023*

- Analisi dei rischi legati a dipendenze software, fornitori e componenti open source.
- Proposta di un modello di valutazione e monitoraggio continuo della catena di fornitura.
- Casi di studio tratti da incidenti reali e indicazioni operative per le PMI.

Progetti

Piattaforma condivisa di threat intelligence — **https://github.com/lorenzobian**

Progetto open source per la condivisione di indicatori di compromissione tra piccole e medie imprese italiane.

- Raccolta e normalizzazione di indicatori di compromissione da fonti eterogenee.
- API per l'integrazione con SIEM e piattaforme di ticketing.
- Documentazione e laboratori per l'adozione da parte di organizzazioni con risorse limitate.

Parole chiave: Threat intelligence, STIX/TAXII, Open source

Laboratorio di penetration testing — **https://github.com/lorenzobianchi/pentest-lab**

Ambiente virtualizzato per esercitazioni su vulnerabilità web e di rete. — *feb 2019–lug 2019*

- Configurazione di macchine vulnerabili e scenari di attacco controllati.
- Sperimentazione di tecniche di enumerazione, sfruttamento e post-sfruttamento.
- Redazione di report con raccomandazioni di correzione.

Parole chiave: Penetration testing, OWASP, Virtualizzazione

Interessi

Sicurezza informatica: CTF, Ingegneria inversa, OSINT

Sport: Corsa, Nuoto, Ciclismo

Lettura: Saggistica, Fantascienza

Volontariato

Security Without Borders Italia **https://www.securitywithoutborders.it**

Volontario e mentore *mar 2019–Presente*

- Mentoring per giovani professionisti e studenti che si avvicinano alla sicurezza informatica.
- Organizzazione di laboratori pratici su phishing, igiene digitale e protezione dei dati.
- Supporto alla community nella gestione responsabile delle vulnerabilità.

Associazione Informatica Solidale **https://www.informaticasolidale.it**

Formatore digitale *ott 2017–dic 2018*

- Corsi di alfabetizzazione digitale e sicurezza online per persone over 60.
- Creazione di materiali divulgativi semplici e accessibili.
- Collaborazione con biblioteche e centri civici del territorio.