

Luca Formosa

LinkedIn: [linkedin.com/in/luca-formosa-775088160/](https://www.linkedin.com/in/luca-formosa-775088160/)

Credly: [credly.com/users/luca-formosa](https://www.credly.com/users/luca-formosa)

PROFILO PROFESSIONALE

Chief Information Security Officer e Cybersecurity & Network Architect con oltre dieci anni di esperienza nel disegno e nella protezione di infrastrutture critiche. Integro firewall multi-vendor (Cisco, Fortinet, Zyxel, ecc), soluzioni SD-WAN e piattaforme EDR/XDR/MDR per garantire performance elevate e continuità operativa in ambienti enterprise distribuiti.

Coordino programmi di Governance, Risk & Compliance traducendo gli standard ISO 27001, NIST CSF e i requisiti GDPR in controlli tecnici misurabili. Conduco assessment di rischio, definisco policy di sicurezza, gestisco audit interni ed esterni e supervisiono la risposta agli incidenti mediante piattaforme SIEM/SOAR, con monitoraggio costante di KPI e KRI.

Collaboro con il Board e i C-level (CEO, CIO, CTO, COO) per sviluppare roadmap di cyber-resilienza allineate agli obiettivi di business, con particolare attenzione al time-to-value e all'ottimizzazione dei costi. Disponibile per consulenze strategiche, porto un approccio orientato alle best practice, alla trasparenza e al miglioramento continuo.

ESPERIENZA PROFESSIONALE

CISO & ICT System Architect

LGK Computer S.r.l. | Ottobre 2014 – Presente | Roma, Italia

- **SIEM & SOAR:** Implementazione di soluzioni per il monitoraggio (SIEM) e l'automazione della risposta (SOAR), riducendo drasticamente i tempi di gestione degli incidenti.
- **MDR, EDR & XDR:** Introduzione di tecnologie di Managed Detection & Response, Endpoint Detection & Response e Extended Detection & Response, garantendo protezione in tempo reale e remediation automatizzate.
- **RMM:** Adozione di strumenti di Remote Monitoring & Management (es. SolarWinds) per manutenzione predittiva e reattiva, riducendo i tempi di fermo.
- **Network Architecture & SD-WAN:** Progettazione di topologie di rete (VLAN, subnet, WAN link) e utilizzo di soluzioni SD-WAN per migliorare la connettività su più sedi.
- **Firewall & Intrusion Prevention:** Configurazione e ottimizzazione delle policy firewall (Zyxel, Cisco, Fortinet), con aggiornamenti IDS/IPS per far fronte a minacce in continua evoluzione.
- **Compliance & Best Practice:** Rispetto degli standard ISO 27001 e NIST, con periodiche revisioni e miglioramenti incrementali per anticipare attacchi sofisticati.
- **Gestione Progetti & Documentazione:** Coordinamento delle fasi di progetto, dal Proof of Concept (PoC) alla messa in produzione, e redazione di High-Level Design (HLD) e guide tecniche.

ICT System Architect Senior & Information Security Auditor

Gruppo Distribuzione S.p.A. | Giugno 2021 – Novembre 2024 | Roma, Italia

- Supervisione di firewall e sicurezza di rete su nove sedi, definendo policy e procedure su Zyxel, Cisco e Fortinet.
- Implementazione di FortiClient EMS (policy off-fabric) e successiva migrazione a Sangfor EDR, migliorando la protezione degli endpoint.
- Adozione di soluzioni SD-WAN, segmentazione avanzata e multi-perimetro per potenziare connettività e ridondanza.
- Migrazione degli ambienti Windows Server (da 2012 a 2019) e consolidamento dei domini aziendali.
- Installazione di sistemi SIEM (SGBox, CyberCommand, FortiAnalyzer, ecc) per analisi dei log in tempo reale e risposta automatizzata alle minacce, in linea con ISO 27001.
- Definizione di procedure operative e audit interni per mantenere best practice e conformità alle normative vigenti.

IT Manager

Pubblitoni S.r.l. | Novembre 2010 – Ottobre 2014 | Roma, Italia

- Gestione infrastruttura IT, inclusa l'integrazione di macchinari di grande formato in rete.
- Migrazione e ottimizzazione dei sistemi gestionali, con una riduzione dei costi operativi e maggiore efficienza produttiva.
- Ideazione di un foglio di calcolo avanzato per la gestione di 5.000 manifesti pubblicitari, migliorando il controllo e l'organizzazione del materiale.
- Collaborazione con fornitori esterni per l'introduzione di soluzioni innovative, riducendo costi e tempi di inattività.

Protocol Officer

Ministero della Difesa – C.I.T.S. | Marzo 2009 – Ottobre 2010 | Pratica di Mare, Italia

- Gestione di protocolli operativi, servizio mensa e posta classificata, rispettando rigorosi criteri di sicurezza e riservatezza.
- Compilazione di documentazione amministrativa e supervisione dei processi di autorizzazione, ottenendo encomi per l'accuratezza e la dedizione.

ISTRUZIONE E FORMAZIONE

- **CCIE Security** – in corso – Nitiz Sharma
- **CISO Course** – CybersecurityUp / Fata Informatica (2024)
- **Corso ICS2 CISSP** – Elis Formazione (completato nel 2023)
- **Micromaster in Cybersecurity** – Rochester Institute of Technology (RIT), USA (Gennaio 2020 – Ottobre 2020)
- **Diploma in Ragioneria e Programmazione** – IIS Leonardo da Vinci, Roma

CERTIFICAZIONI

- **Certified Information Security Officer (CISO)** – CybersecurityUp / Fata Informatica (2024)
- **CCNP Security** – Cisco (2024)
- **PenTest+** – CompTIA (2021)
- **VCP-DCV 7.0** – VMware (2021)
- **CCNP Routing & Switching** – Cisco (2019)
- **CCNA Security** – Cisco (2019)
- **CCDA** – Cisco (2019)
- **CCNA Routing & Switching** – Cisco (2018)

COMPETENZE

- **Firewall & Network Security:** Configurazione e gestione (Zykel, Cisco, Fortinet), IDS/IPS
- **SIEM & SOAR:** Analisi degli eventi di sicurezza, risposta automatizzata agli incidenti
- **Endpoint Protection:** EDR, XDR, MDR; sicurezza degli endpoint e gestione centralizzata
- **SD-WAN & Networking:** VLAN, subnetting, WAN link, infrastrutture scalabili e ad alta disponibilità
- **Compliance:** ISO 27001, NIST Cybersecurity Framework
- **Project Management:** Gestione di progetti complessi, dal Proof of Concept al rilascio in produzione
- **Documentazione Tecnica:** High-Level Design (HLD), manuali operativi e guide tecniche
- **RMM:** Implementazione e gestione di piattaforme di monitoraggio remoto (SolarWinds)
- **Soft Skills:** Comunicazione interfunzionale, problem solving, flessibilità oraria

ALTRE INFORMAZIONI

- **Lingue:** Italiano (madrelingua), Inglese (B2), Spagnolo (A1)
- **Interessi:** Viaggi, tecnologie innovative, progetti di laboratorio (PoC)
- **Patente:** Categoria B

DICHIARAZIONE SULLA PRIVACY

Autorizzo il trattamento dei miei dati personali ai sensi della normativa vigente in materia di protezione dei dati. Dichiaro che le informazioni riportate nel presente CV sono veritiere e verificabili.