

INFORMAZIONI PERSONALI

Morsicani Riccardo (Italia)

DICHIARAZIONI PERSONALI

Professionista dell'Information Technology e della sicurezza con oltre 20 anni di esperienza nella progettazione e implementazione di soluzioni Identity Management, Provisioning e De-Provisioning / Identity Workflow, Cyber Security, Security Audit e Penetration Testing, SIEM Technologies, LDAP Directories, Enterprise System Architecture, Security Infrastructure Design, Autenticazione e tecnologie di autorizzazione, oltre a framework di sicurezza e tecnologici personalizzati. Ho esperienza, tra gli altri, nel settore bancario, assicurativo, governativo, farmaceutico e delle telecomunicazioni.

ESPERIENZA
PROFESSIONALE

2023–alla data attuale

Managing Director

Key Partner Cyber

Responsabile del centro di eccellenza in cyber security del gruppo Key Partner

2019–2023

Principal Security Architect - Presales Manager

Cybertech

Come Responsabile del Presales, coordino l'area di prevendita (Incontri con i clienti, raccolta requisiti, redazioni offerte, redazioni stime tecniche, risposta a gare, progettazioni campagne) e l'interfaccia con l'area commerciale e il management (report, KPI, forecast ecc.)

Come architetto senior, seguo l'analisi e la progettazione di soluzioni tecnologiche per clienti large enterprise

2017–2019

Principal Security Architect - Presales Manager

OmnitechIT

Come Responsabile del Presales, coordino l'area di prevendita (Incontri con i clienti, raccolta requisiti, redazioni offerte, redazioni stime tecniche, risposta a gare, progettazioni campagne) e l'interfaccia con l'area commerciale e il management (report, KPI, forecast ecc.)

Come architetto senior, seguo l'analisi e la progettazioni di soluzioni tecnologiche per clienti large enterprise

2014–2016

Security Architect - Research & Development Manager

OmnitechIT

- Progettazione di soluzioni di sicurezza complesse per clienti enterprise principalmente in ambito Identity access and Governance, SIEM e MSS, sia in Italia che all'estero (settore Bancario, assicurativo, pubblica amministrazione, telecomunicazioni, automotive ecc.; alcuni esempi: BNL – BNP Paribas, EVRY in Posetn (Oslo – Norway), Samba Bank (Riyad - KSA), Nahdi (Jeddah – KSA), Garanti Bank (Istanbul – Turkey), CMA (Kuwait), EVERIS in AXA-Securos (Madrid – Spain), ecc.)

- Come Responsabile dell'area ricerca e sviluppo, progettazione e coordinamento dei progetti interni di ricerca; sviluppo delle proposizioni di offering in ambito Cyber Security, Industry 4.0 and IoT,

Blockchain.

2009–2016 Security Analyst

OmnitechIT, Roma

- Esecuzione di security audit (penetration test, vulnerability assessment, web application PT) presso piattaforma applicative e sistemistiche del cliente, con utilizzo di metodologie OSSTMM e OWASP
- Esecuzione di compliance audit
- Redazione report dettagliato delle attività di audit e dei rilievi effettuati.

2007–2014 Senior Security Consultant

Omnitechit

Presso clienti come: Telecom Italia, Sara Assicurazioni, Notartel, Alitalia, Hp Dcs, Vodafone It, AVCP, Ministero della Giustizia, Ministero dell'Interno, ENEL energia, Gruppo Generali, Banca IntesaSanpaolo, Legambiente

- Progettazione e integrazione di infrastrutture SIEM (Novell, RSA, IBM, CA ecc.) con definizione di modelli di monitoraggio, indicatori di performance di rischio, regole di correlazione, sviluppo di componenti custom ecc.
- Progettazione e realizzazione di infrastrutture di HA, Virtualizzazione e Mail Delivery, difesa perimetrale ecc

2006–2007 Security Consultant

OmnitechIT, Roma

Progettazione ed Implementazione di architetture SIEM (Security Information Event Management), mediante personalizzazione del prodotto Novell Sentinel 6.

Realizzazioni orientati alla compliance tecnologica con la normativa 196/2003 e successive variazioni.

ISTRUZIONE E FORMAZIONE

2023 CISM Certified Information Security Manager

ISACA

2022 ITIL V4 Foundation

AXELOS Global Best Practice

2014 IBM Security QRadar SIEM v7.1 Implementation

IBM

2012 RSA SE Associate in Security Management

RSA Security

•

2010 Ethical Hacker

Unidata S.p.A, Roma

- Laboratorio avanzato per Security Auditor, tecniche e metodologie di audit e di penetration test.

- 2011 **OSSTMM Professional Security Tester**
ISECOM
Corso su metodologia di analisi di sicurezza OSSTMM, teorica e pratica
- 2007 **Procedure ISMS (Information Security Management System)**
Telecom Italia, Roma
 - Sistema documentale ISMS, procedure operative ISMS;
 - Norma ISO/IEC 27001:2005
- 2006 **Tecnico informatico – Security Manager (30/30)**
Centro Manuela Mezzelani, Roma
 - Corso avanzato di sicurezza informatica
- 1998–2002 **Laurea in Filosofia (110 e lode)** Livello 6 QEQ
Università “La Sapienza”, Roma (Italia)

COMPETENZE PERSONALI

Lingua madre italiano

Lingue straniere

inglese

COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
Ascolto	Lettura	Interazione	Produzione orale	
C1	C1	B2	B2	B1

Livelli: A1 e A2: Utente base - B1 e B2: Utente autonomo - C1 e C2: Utente avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

• Ottime competenze comunicative e divulgative acquisite durante la decennale esperienza come consulente e prevenditore, supportate dalla capacità di relazionarsi con interlocutori di diverso livello (tecnici e business).

Competenze organizzative e gestionali

• Leadership e competenze organizzative (attualmente responsabile del team di prevendita, segue la parte di organizzazione del lavoro, e di reporting al top management)
• Buone capacità di team-leading e di coordinamento tecnico acquisite nel ruolo di architetto di soluzioni IT.

Competenze professionali

• Ottime capacità di raccogliere, comprendere e organizzare i requisiti di business, funzionali e tecnici dei clienti, acquisite durante l'esperienza di consulente ed architetto e perfezionate come prevenditore

Competenze digitali

IBM Security QRadar SIEM V7.1 Implementation
RSA SE Associate in Security Mgt
OSSTMM Professional Security Tester (OPST)
Rational Application Developer Technical Sales Professional
Novell Certified Linux Professional (Novell CLP)
Novell Certified Linux Administrator (Novell CLA)
Novell Security and Identity Management Technical Specialist

Security

Conoscenza tecnica approfondita di:

- SOC/SIEM (Security Information Event Management) – Novell Sentinel, RSA en Vision, IBM Tcim, IBM qRadar, splunk, Demisto, IBM Resilient

- Hardening

- Firewall (Cisco IOS, Netfilter/Iptables, Check Point)

- IDS (IBM ISS, Tipping Point)

- IAM (CA Identity Suite, IBM ISIM/IGI, IBM TAM/ISAM)

Conoscenza funzionale della tematica e dei principali prodotti di mercato nelle seguenti aree:

IAaG (Identity Access and Governance), Advanced and Risk based Authentication, SIEM (Security Information and Event Management) , Privilege Account Management, Vulnerability and Penetration Testing, SOAR (Security Orchestration Automation and Response), Network Security, EDR (Endpoint Detection and Response), Security Intelligence and Analytics, Cloud infrastructure and Cloud Security, Data Protection and Governance.

Sistemi Operativi

Microsoft Dos, Windows 98/ME/XP/8/10/2000/NT/Vista/2003/2008/2012,
*nix based system, Mac OsX

Database

Oracle, Microsoft SQL Server, MySQL, Postgres, Linguaggio SQL, LDAP

Programmazione

Bash Scripting, linguaggio C, Dos Batch, Php, ActioScript 2.0, Novell RuleLg, Html, Javascript, Node.js, Java (base)

Networking

design/gestione LAN, HA, Clustering & LB, Cisco IOS, hosting

Application Sever

WebServer (Apache, Microsoft IIS), DC, DNS, WINS, DHCP

Application

Xen Virtualization, Hearbeat, LSV, Postix, CourierMail, Dovecot ecc

Security Audit

Metodologie OWASP, OSSTMM

Security Audit tools

Tutti i principali strumenti per Vulnerability Assessment e Penetration Test, tra cui Kali, Nmap, Httprint, Wireshark, hping, Nikto, nessus, John the ripper, Hydra, Medusa, Cain, Rainbowcrack, Webscarab, Burp, HP WebInspect, Metasploit Framework, Fortify, APPscan.

GRC (Governance Risk and Compliance)

Principali normative e best practices internazionali, tra cui PCI-DSS, GDPR, PSDII, ISO 27001, TOGAF, ITIL