

ANTONIO DAVOLI

Electronics engineer with extensive experience on cybersecurity, telecom and ICT domains



+39 3280623996



<https://www.antoniodavoli.it/>



<https://www.linkedin.com/in/antoniodavoli/>



davoli.antonio@gmail.com



Rome (Italy)



1964



EXPERIENCE

Mead Informatica

2022-2025 • Roma

I carried out cybersecurity activities for customer corporates

Sisal Entertainment

(as external consultant) 2019-2021 • Roma

I managed projects on web portal for online betting

Gruppo Delco Spa (Comapp)

2000-2018 • Roma

I managed projects and accounts on VoIP and Contact Center

Gruppo Telecom Italia (Saritel)

1996-2000 • Roma

I designed, sold and managed projects on PSTN Telecom Value Added Systems and Services

Gruppo Finmeccanica (Alenia)

1992-1995 • Roma

I carried out Unix mainframes and LAN administrator activities

Biotronix

1990-1992 • Roma

I developed software on marine pollution and bioengineering

EDUCATION

Cyber Security University Master's Degree

103/110

"La Sapienza" University of Rome

2018 - 2021 • Roma

Electronics Engineering Master's Degree

110/110

"La Sapienza" University of Rome

1984 - 1990 • Roma

Scientific High School

60/60

"Galileo Galilei"

1978-1983 • Lamezia Terme

Professional Certificates

ISO/27001:2022 Security Lead Auditor Certification 2025- 2025

ISO/27001:2022 Security Risk Manager Certification 2025- 2025

Certified Professional Penetration Tester (eCPPT) 2024- 2024

Junior Penetration Tester (eJPT) Certified 2023- 2023

Sentinel One XDR Singularity Admin Certified 2023- 2023

Claroty/Medigate HealthCare Platform Certified 2022-2023

Armis HealthCare Platform Certified 2022- 2023

PM SCRUM Fundamental Certified 2021- 2021

Certified Ethical Hacker (CEH v10) 2018- 2019

PROJECTS

- ✓ Telemedicine, Sea Pollution, Remote Sensing 1990 – 1995
- ✓ Voicemail and SMS services on mobile/PSTN 1996 – 2000
- ✓ VoIP Unified Communication, Contact Center 2000 – 2018
- ✓ Web Portals for online betting 2019 – 2022
- ✓ Cybersecurity Assessment 2022 – 2025
- ✓ HealthCare SOC 2022 – 2025
- ✓ Cybersecurity Training Awareness 2022 – 2025
- ✓ Phishing Simulation Campaigns 2022 – 2025
- ✓ Vulnerability and Web Application Scan 2022 – 2025

SKILLS

- I carry out **Vulnerability Assessments** (Qualys)
- I simulate **Phishing Campaigns** (Trend Micro, GoPhish)
- I carry out Open-Source Intelligence/**OSINT reconnaissance**
- I carry out **Automated Web App Scan** (Qualys)
- I carry out **HealthCare Compliance Assessments** (Claroty, Medigate, Armis)
- I set up **EDR** platforms and suites (Sentinel One, Trend Micro)
- I am familiar with IT security processes for **SIEMs and SOCs**
- I am familiar with basic techniques of **Network Defense, Ethical Hacking, Malware, Forensic Analysis and Penetration Test**
- I am familiar with frameworks like **ISO 27001, ISA/IEC 62443**,
- I designed IT, data networking and Sip/VoIP/CTI architectures.
- I have extensive **Project Management** experience in the fields of web portals, data networks, telecommunications and cybersecurity.
- I know several programming languages: C++ (basic), C, Pascal, Fortran, VB.NET, Html, Assembly (reading), Python (scripting).

LANGUAGES

Italian

Native (C2)



English

Intermediate (B2)



French

Intermediate (B1)



ACHIEVEMENTS

Key Customers Project Management on "Utility" context

Technical and economic management of TLC solutions and projects in the utility/energy market for a cumulative value of 45 million euros in the period 2000-2018

Key Customers Project Management on "Telco" context

Technical and economic management of TLC solutions and projects in the telecom market for a cumulative value of 5 million euros in the period 2000-2018

Customers Project Management on "Cyber" context

Various cybersecurity solutions in manufacturing, transportation, healthcare, SMEs, in the period 2022-2025

KEY MANAGED CUSTOMERS

Sisal, Enel, Wind, Telecom Italia, Tiscali, Almagora, Trenitalia, American Express, BT, Public HealthCare and other small and medium-sized Italian companies.

I authorize the processing of my personal data pursuant to GDPR 679/16