CONTATTI

- Taranto (TA), Italia
- +39 333 904 6852
- dennisepede@proton.me
- linkedin.com/in/dennis-sepede-cybersecurity
- github.com/Den-Sec
- securitixsolutions.com
- dennissepede.com

COMPETENZE

Offensive & AI Security
Pentest Web/Mobile/AI-LLM · Red Teaming · prompt injection/guardrail bypass · Exploit/PoC dev · Burp Suite Pro · Nessus

Vulnerability Research
CVE & advisory · Coordinated disclosure · Bug bounty

Threat Intelligence
CTI · OSINT / SOCMINT · threat hunting

Detection & Response
XDR/EDR (ESET, Wazuh) · SIEM · IPS/IDS · DFIR & forensics (Velociraptor, IRIS, Autopsy, Wireshark) · MISP

GRC & Compliance
ISO/IEC 27001 · NIS2 · GDPR · risk management

Cloud & DevSecOps
AWS · Proxmox · Docker · Cloudflare · Zero Trust (M365/AD) · CI/CD · SAST/DAST

Python · Go · TypeScript · C++ · Bash · PowerShell · PostgreSQL · MongoDB · Redis · Elastic

CERTIFICAZIONI

AWS Cloud Practitioner
CLF-C01 · 2023

CompTIA Security+
SY0-601 · 2022

LINGUE

Italiano — Madrelingua

Inglese — C1 Advanced

Spagnolo — Intermedio

DISPONIBILITÀ

Mobilità: globale · **Impegno:** full-time
NDA e security clearance.

Dennis Sepede.

Cybersecurity Leader · CTO & Co-Founder

Offensive Security · AI Security Research · Threat Intelligence

PROFILO

Cybersecurity leader formato negli Stati Uniti su infrastrutture critiche, a fianco di dirigenti del Pentagono, con esperienza nella guida della sicurezza in contesti industriali enterprise. Come Co-Founder & CTO di Securitix Solutions e CTO di Vulneralt progetto e sviluppo end-to-end piattaforme proprietarie di difesa, dall'XDR/MDR alla Cyber Threat Intelligence con AI.

Costruisco la sicurezza su **tre pilastri che porto in ogni contesto**. Sul fronte della **governance** traduco standard come ISO/IEC 27001 e NIS2 in procedure operative e negli strumenti che le rendono vive, non in documenti che restano nel cassetto. Sui **processi** orchestro detection & response, vulnerability management e hardening capaci di reggere l'attacco reale. E la **formazione** è il pilastro in cui credo di più: la coltivo su me stesso e la costruisco per gli altri, dai programmi di awareness alle piattaforme di formazione che ho sviluppato, fino al mentoring di team e studenti.

Ricercatore prima ancora che dirigente: **oltre 40 vulnerabilità segnalate** in coordinated disclosure, con **CVE Critical assegnate**, su programmi enterprise tra cui Grafana, GitLab e Anthropic, con un focus crescente sull'**AI security**, l'area dove l'AI non è solo difesa ma diventa essa stessa superficie d'attacco - dove sono **tra i primi approvati nel Cyber Verification Program di Anthropic** per la security offensiva a duplice uso. A.A.S. in Cybersecurity con lode negli USA e membro della **Phi Theta Kappa Honor Society**; certificazioni AWS e CompTIA, speaker su AI & cybersecurity.

ESPERIENZA

Cybersecurity Operations & Engineering Manager — Lug 2023 - oggi

Comes S.p.A. - costruzioni e ingegneria industriale · Italia

- **Direzione della sicurezza**: guido l'intera funzione come unico referente interno del gruppo, dalla strategia agli standard fino all'esecuzione operativa.
- **Security operations**: dirigo il team tecnico interno e il monitoraggio MDR esterno, con interventi diretti su firewall, EPP/XDR, hardening e pentest interni.
- **Governance & compliance**: conduco l'adeguamento NIS2 e il percorso ISO/IEC 27001 come responsabile interno, coordinando il fornitore esterno specializzato.
- **Sviluppo & self-hosting**: progetto e deployo lo stack proprietario (Valta CTI, Mirage) e un password filter LSA custom, con servizi self-hosted (OpenSign, Moodle, Vaultwarden, Ollama) sotto controllo diretto.
- **Identità & accessi**: metto in sicurezza Active Directory e Microsoft 365 in ottica Zero Trust (Conditional Access, DLP).
- **Awareness & formazione**: formo il personale su cyber e AI con video, sessioni in presenza ed email, phishing simulation e mentoring.

IMPRENDITORIA & LEADERSHIP

Co-Founder & CTO – Securitix Solutions

2024 - oggi

> La difesa la costruisce chi sa come si attacca: **MSSP italiano** che protegge le imprese regolate con **tecnologia propria**, non rivenduta dall'estero - «Difendiamo chi costruisce».

- **Responsabile dell'intero lato tecnico e di prodotto**: ho progettato e portato in produzione **9 piattaforme proprietarie**, dall'architettura al deployment multitenant - una **suite integrata per design**, non un collage di prodotti acquisiti.
- Selezionato al **Google for Startups Cloud Program** (**$25.000** in crediti R&D) e **partner nel Claude Partner Network di Anthropic**.
- **Servizio di sicurezza gestita** end-to-end - detection & response, hardening e compliance - con **dati e operatività in Italia**.
- Collaborazioni di ricerca con **Università del Salento** e **CRISR** su resilienza cyber.
- Governance **security-by-design**: percorsi **ISO/IEC 27001, NIS2 e GDPR** per piattaforma e clienti.

CTO – Vulneralt

2025 - oggi

> La sicurezza enterprise resa **accessibile e sartoriale** per le PMI: meglio un passo piccolo fatto bene che una piattaforma fuori portata, protezione mai sovradimensionata.

- **Cyber risk assessment**: analisi dell'esposizione (credenziali, rete, email, dispositivi) e compliance GDPR/NIS, con report azionabili.
- **Monitoraggio continuo 24/7** con alert in tempo reale e remediation quick-win.
- **Advisory, formazione e supporto continuo**, in partnership con l'IT del cliente, su misura per le PMI.

PRODOTTI & R&D (SECURITIX)

Suite proprietaria progettata e sviluppata end-to-end - la tecnologia su cui Securitix opera il servizio gestito, costruita in casa e non importata:

Presidio XDR — XDR/MDR · flagship

SOC multitenant erogato come servizio: detection & response con playbook SOAR, DFIR (IRIS), threat intelligence (MISP) e dashboard Grafana, su stack Wazuh + Velociraptor.

Valta CTI — Threat Intel

Threat intelligence con AI: correla IoC da fonti multiple, con scoring di rilevanza, arricchimento automatico e gamification per gli analisti.

Mirage — Deception

Honeypot e deception AI-driven: esche e sensori realistici per intercettare i movimenti laterali, integrati nativamente con Presidio.

Tempest — Stress test

Stress tester di rete in Go: 17 engine L7/L4 per misurare resilienza e capacity di applicazioni e infrastrutture sotto carico.

PhishSim — Phishing

Phishing simulation completa: 80 template email e 40 landing page, con tracking delle interazioni e reportistica di awareness.

Forge — Training

LMS brandizzato su Moodle: awareness B2B, formazione tecnica certificata e percorsi AI, per clienti e team interni.

Ransomware Simulator — Awareness

Simulatore educational in Go: riproduce in sicurezza la catena d'attacco ransomware per dimostrare le difese nei seminari di awareness.

Cipher — Risk · WIP

Matrice di rischio cyber per PMI (in sviluppo), bilingue IT/EN: scenari di rischio per settore e raccomandazioni prioritizzate.

Sign — e-Signature

Firma documentale self-hosted su Documenso: firma elettronica, gestione template e audit trail completo, sotto controllo del cliente.

Argus — AIOps · WIP

AIOps co-pilot per PMI/MSP (in sviluppo): aggrega la telemetria IT, produce diagnosi assistite da AI e suggerisce azioni guidate.

SECURITY RESEARCH & CVE

3	4	10	+40
CVE CRITICAL ASSEGNATE	CVE IN ATTESA MITRE	ADVISORY PUBBLICATE	TARGET ENTERPRISE

CVE-2026-38595
im3x/Scriptables · Critical
OS Command Injection: comandi arbitrari sull'host via input non sanitizzato.
CWE-78

CVE-2026-38600
gohttpserver · Critical
Path Traversal / Zip Slip: scrittura di file fuori dalla cartella di estrazione.
CWE-22

CVE-2026-38601
gohttpserver · Critical
Hard-coded Credentials: sessioni forgiabili da segreto statico nel codice.
CWE-798

IN ATTESA DI ASSEGNAZIONE MITRE

YoutubeDL-Material
Argument Injection
CWE-88

Youtube-dl-REST
OS Command Injection
CWE-78

ChatGPT-Web
Deserializzazione insicura
CWE-502

agent-studio
Deserializzazione insicura
CWE-502

- **10 advisory di coordinated disclosure** (repo **Den-Sec/security-research**): un **cross-origin header leak** ricorrente su **6 librerie HTTP client** (undici, node-fetch, follow-redirects, go-resty, req, gorequest), piu' i finding su gohttpserver e im3x poi assegnati come CVE.
- **Bug bounty e vulnerability research su 40+ target** via Bugcrowd, Intigriti, HackerOne e Huntr, su programmi enterprise tra cui **Grafana, Aiven, MLflow, AWS SageMaker, GitLab, Nextcloud**, con **finding riconosciuti e validati dai vendor**.
- **AI-safety research** su **Anthropic** Claude Code (guardrail degradation documentato) e ricerca offensiva su **AI/LLM**: prompt injection, guardrail bypass, agent & pipeline security.

SPEAKING & PUBBLICAZIONI

2026 **Speaker** - **Salone Mediterraneo dell'Impresa** (Confcommercio Taranto), panel *"L'orizzonte digitale del Mezzogiorno: AI, cybersecurity e innovazione per le PMI del Sud"*, in panel con un Analista della **Presidenza del Consiglio dei Ministri** e i vertici nazionali Assintel.

2026 **Tutor dell'Innovazione** - Factory Confcommercio (Taranto), incubazione startup *"Resto al Sud 2.0"*: mentoring di 13 studenti nello sviluppo di un'impresa, con pitch finale a giuria.

2025 **Intervento alla Fondazione Taranto** per la selezione di Securitix al **Google for Startups Cloud Program**: presentazione dell'azienda e dell'impiego dei crediti.

2025 **Seminario di Cyber Threat Intelligence** presso l'**Università di Bari Aldo Moro** (~40 studenti, III anno Informatica).

2025 Autore dell'ebook *"Blueprint di Digitalizzazione Sicura"*.

RICONOSCIMENTI

- **National Cyber League** (USA) - **top 6% nazionale** (381/6273), Forensics 99° percentile · 2023
- **Mid-Atlantic CCDC** (USA) - **16° posto assoluto** · 2023
- **Phi Theta Kappa Honor Society** (USA) - membro · 2023
- **Dean's List · High Honors** (GPA 3.75) - College of Southern Maryland · 2022-2023
- **Gazzetta del Mezzogiorno** - feature su cybersecurity e innovazione (visibilità mediatica regionale) · 2025
- **Tesoriere CyberSec Club**, College of Southern Maryland - 15+ workshop organizzati · 2022-2023

PROGETTI

Progetti di R&D personali tra AI/ML, IoT e security engineering, dall'ideazione al prototipo funzionante:

PasswordFilterDLL Defensive · C++

Password filter LSA per Active Directory (C++): blocca password compromesse (breach-list offline HIBP/Bloom), complessità custom e blacklist, con event logging e deploy GPO. Core unit-testato in CI.

GlubLM AI · ML

LLM da 36M parametri addestrato da zero in PyTorch (test perplexity 3.28), pubblicato su HuggingFace e PyPI; demo PWA on-device via ONNX. R&D su training e model security.

BLOOMPOT AI · IoT

Vaso intelligente **Cyber-Physical System**: telemetria real-time, analisi predittiva AI e sicurezza IoT/Cloud. Lead del team e gestione della roadmap.

TaskPilot Full-stack · PWA

Task manager PWA full-stack (Next.js, PostgreSQL, Prisma, NextAuth): aggiornamenti real-time via SSE, push notifications web, multi-lingua (i18n) e installabile come app, in produzione self-hosted.

ESPERIENZA PRECEDENTE

IT Management Technology Technician - College of Southern Maryland · La Plata, MD (USA) · Gen - Giu 2023
Gestione e supporto dell'infrastruttura IT del campus: troubleshooting hardware/software, manutenzione dei sistemi e supporto agli utenti.

IT Customer Support Technician - 6ya · Remote (USA) · Set 2020 - Giu 2021
Supporto tecnico da remoto ai clienti: diagnosi e risoluzione di problemi hardware e software on-demand.

FORMAZIONE

A.A.S. e Certificate in Cyber Security - College of Southern Maryland (USA) · 2023
Coursework: Ethical Hacking · Digital Forensics · Computer Security · Information Systems Security · Cloud Computing · Linux · Windows Server & Active Directory · Network & Infrastructure Design.

Cisco CCNAv7 (NetAcad) - Introduction to Networks · Switching, Routing & Wireless Essentials · Enterprise Networking, Security & Automation · College of Southern Maryland · 2022-2023

Anthropic - corsi: Claude with the Anthropic API, Claude Code in Action, Introduction to Model Context Protocol, Introduction to Agent Skills · 2026