Smart Cyber Lab

Laboratorio di Cybersecurity

- Marco Motta - Cyber Security Specialist
- Founder & CTO at Globsit srl (Italian Security Provider)
- motta@globsit.com
- @motta (X|twitter account)
- linkedin.com/in/marcomotta (In account)

THE CLASSIC WORK
NEWLY UPDATED AND REVISED

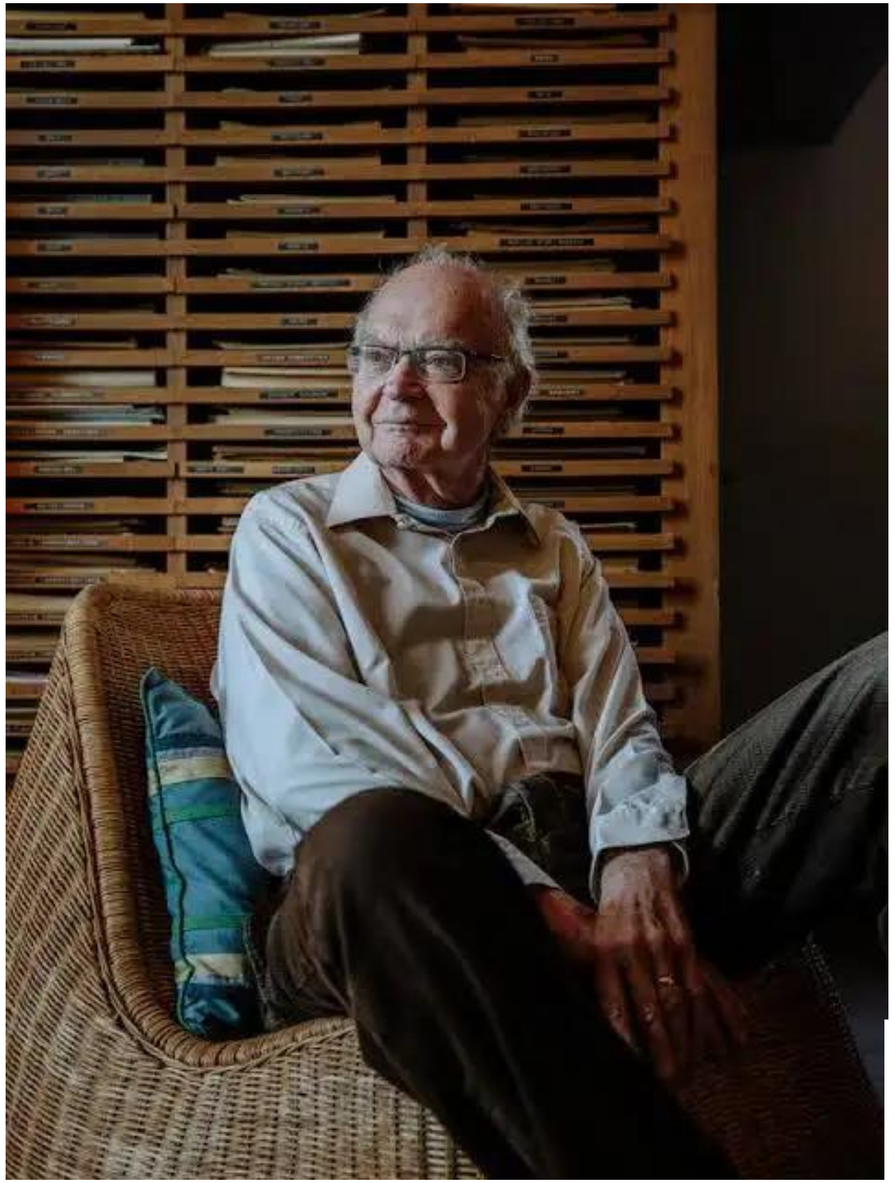
The Art of Computer Programming

VOLUME 1

Fundamental Algorithms

Third Edition

DONALD E. KNUTH



Claude's Cycles

Don Knuth, Stanford Computer Science Department
(28 February 2026; revised 06 March 2026)

Shock! Shock! I learned yesterday that an open problem I'd been working on for several weeks had just been solved by Claude Opus 4.6 Anthropic's hybrid reasoning model that had been released three weeks earlier! It seems that I'll have to revise my opinions about "generative AI" one of these days. What a joy it is to learn not only that my conjecture has a nice solution but also to celebrate this dramatic advance in automatic deduction and creative problem solving. I'll try to tell the story briefly in this note.

Here's the problem, which came up while I was writing about directed Hamiltonian cycles for a future volume of *The Art of Computer Programming*:

> Consider the digraph with m^3 vertices ijk for $0 \le i, j, k < m$, and three arcs from each vertex, namely to i^+jk, ij^+k, and ijk^+, where $i^+ = (i+1) \bmod m$. Try to find a general decomposition of the arcs into three directed m^3-cycles, for all $m > 2$.

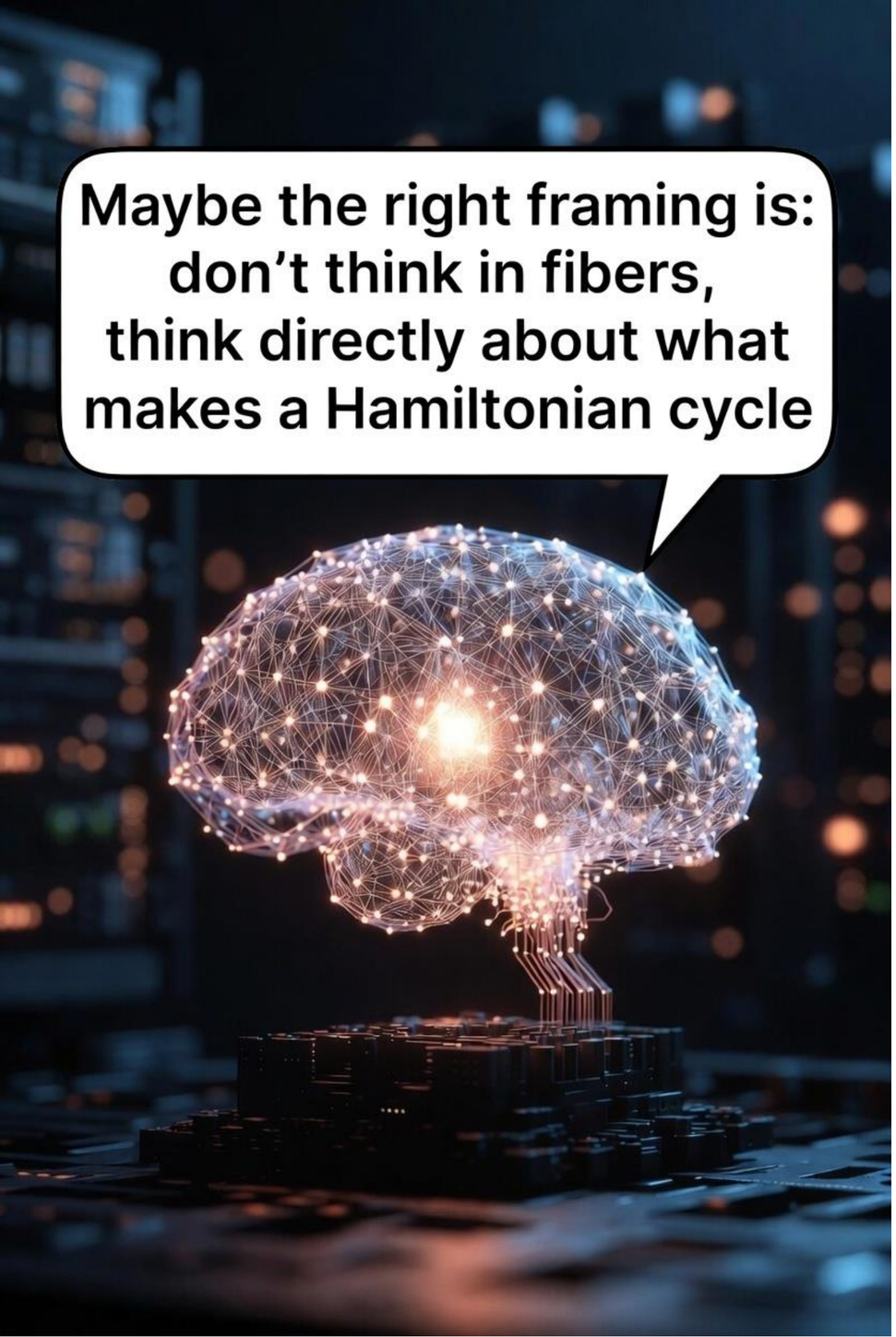
I had solved the problem for $m = 3$, and asked for a generalization as part of the answer to an exercise in [3]. My friend Filip Stappers rose to the challenge, and empirically discovered solutions for $4 \le m \le 16$; therefore it became highly likely that the desired decompositions do exist, except when $m \le 2$.

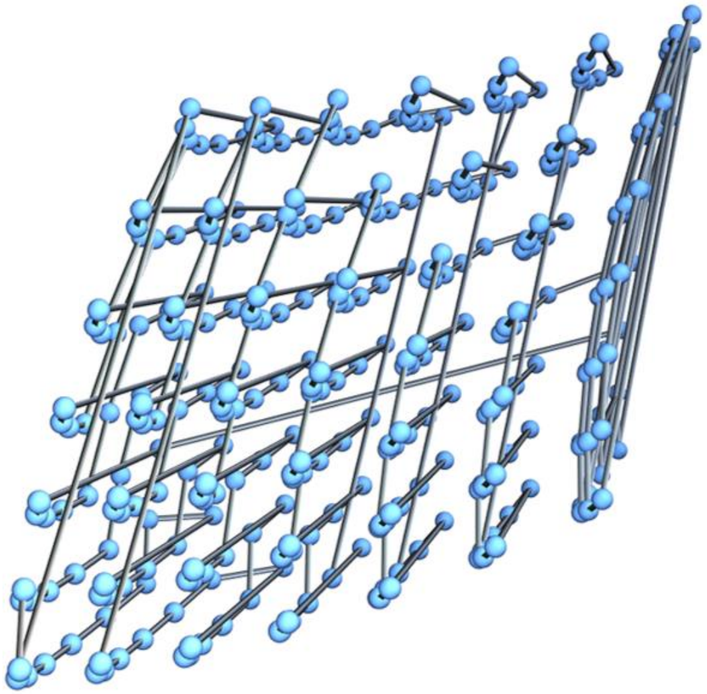
Indeed, it was Filip who had the gumption to pose this question to Claude, using exactly the wording above. He also gave guidance/coaching, instructing Claude to summarize its ongoing progress:

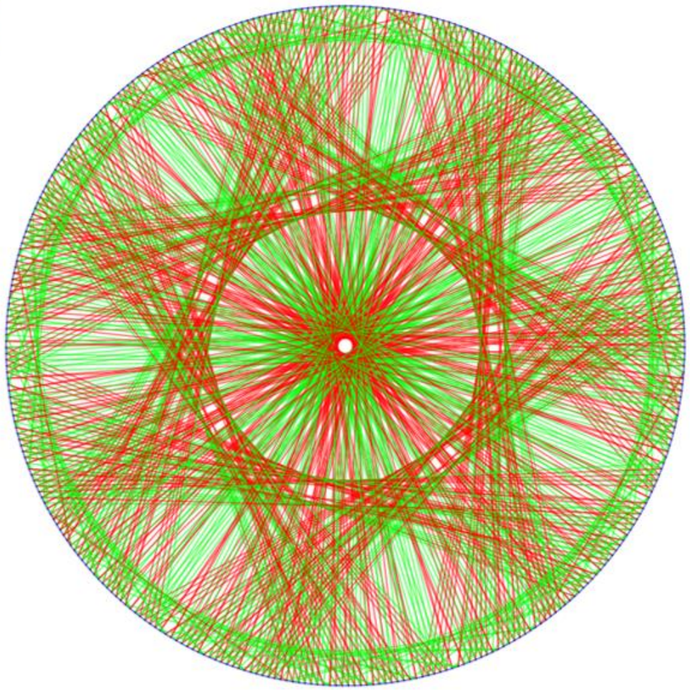
> ** After EVERY `exploreXX.py` run, IMMEDIATELY update this file [`plan.md`] before doing anything else. ** No exceptions. Do not start the next exploration until the previous one is documented here.

And Claude's plan of attack was quite admirable. First it reformulated the problem: "Need sigma: $Z_m^3 \to S_3$, assigning a permutation of $\{0, 1, 2\}$ at each vertex; cycle c at vertex v goes in direction sigma$(v)[c]$. Each

https://www-cs-faculty.stanford.edu/~knuth/papers/claude-cycles.pdf


Maybe the right framing is:
don’t think in fibers,
think directly about what
makes a Hamiltonian cycle





Netsukuku
<<#! wired ;;

FREAKNET

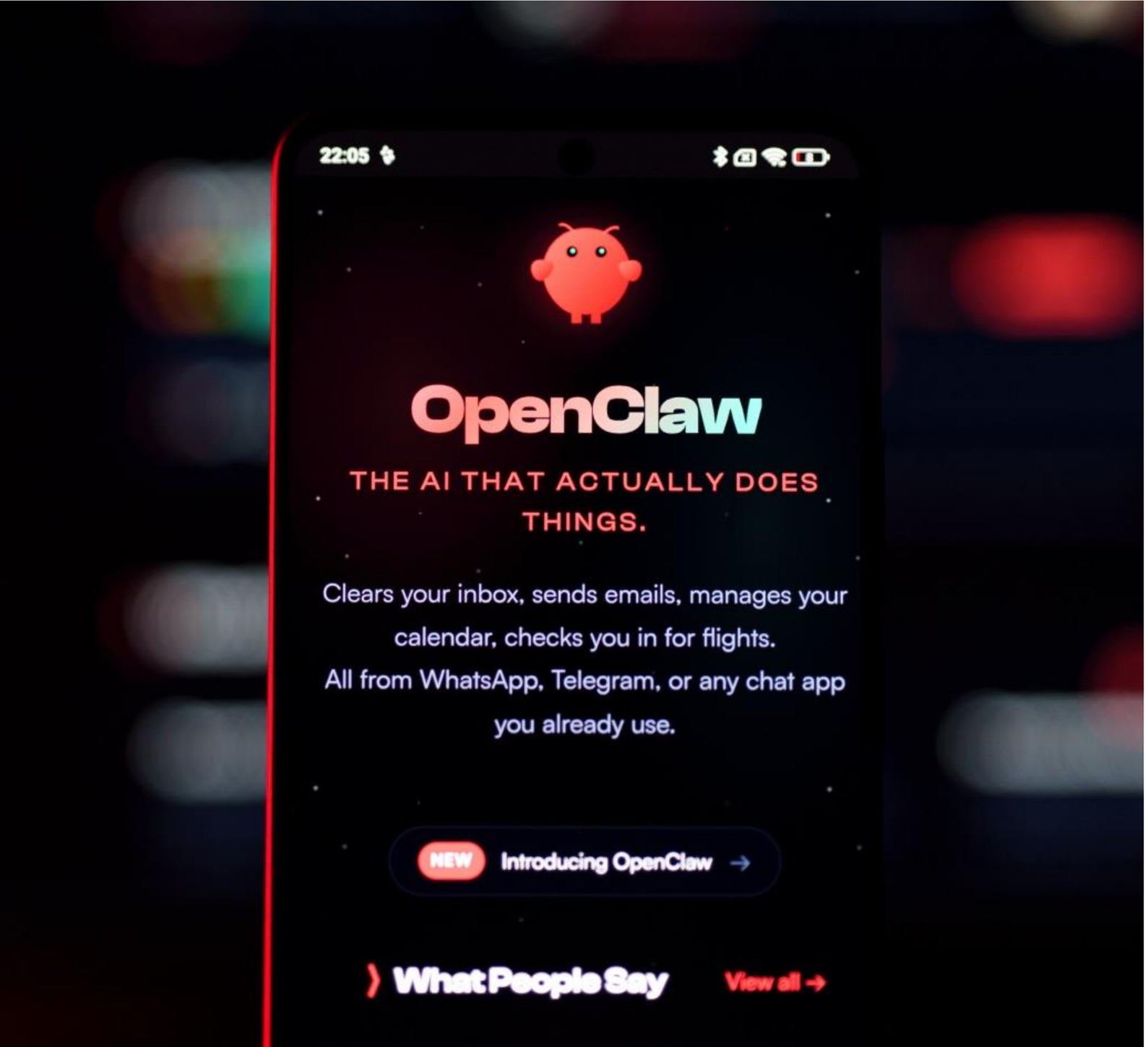
https://netsukuku.freaknet.org/doc/main_doc/qspn.pdf

Claude ha dimostrato che un sistema AI è oggi in grado di esplorare spazi di problema aperti, trovare la riformulazione giusta, e sbloccare in un'ora ciò su cui i ricercatori lavoravano da anni.

Questo cambia radicalmente il modo in cui un attaccante può sviluppare nuove tecniche, e di conseguenza il modo in cui un difensore deve prepararsi.

Gli strumenti di formazione in cyber security non possono ignorare questo nuovo paradigma

L'AI è diventata un vantaggio per gli avversari e la nuova superficie di attacco aziendale!



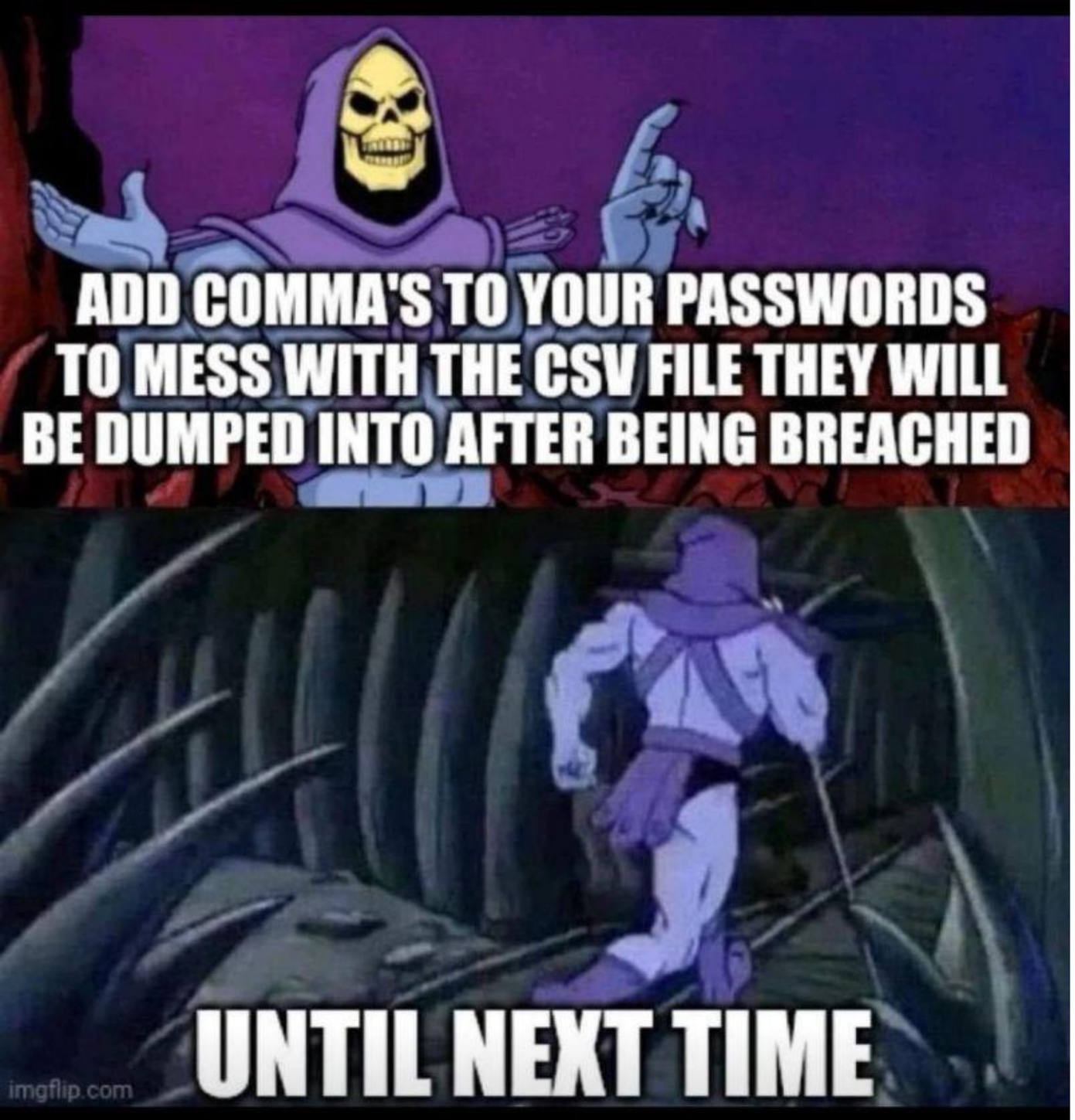
ClawJacked

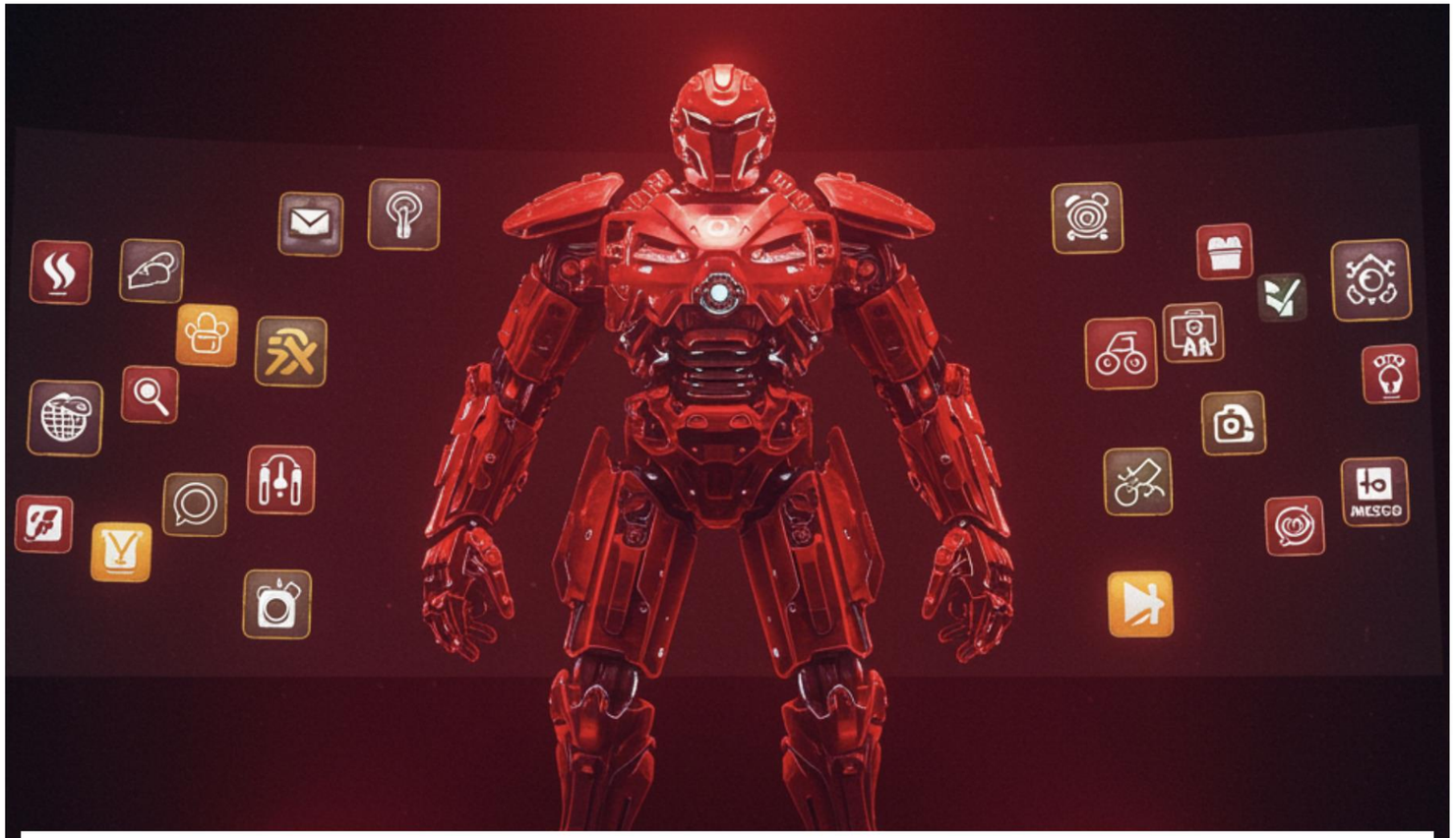
quando un sito web prende il controllo del tuo agente AI

OpenClaw, come molti altri strumenti di sviluppo locale, opera su un'assunzione implicita: se una connessione arriva da

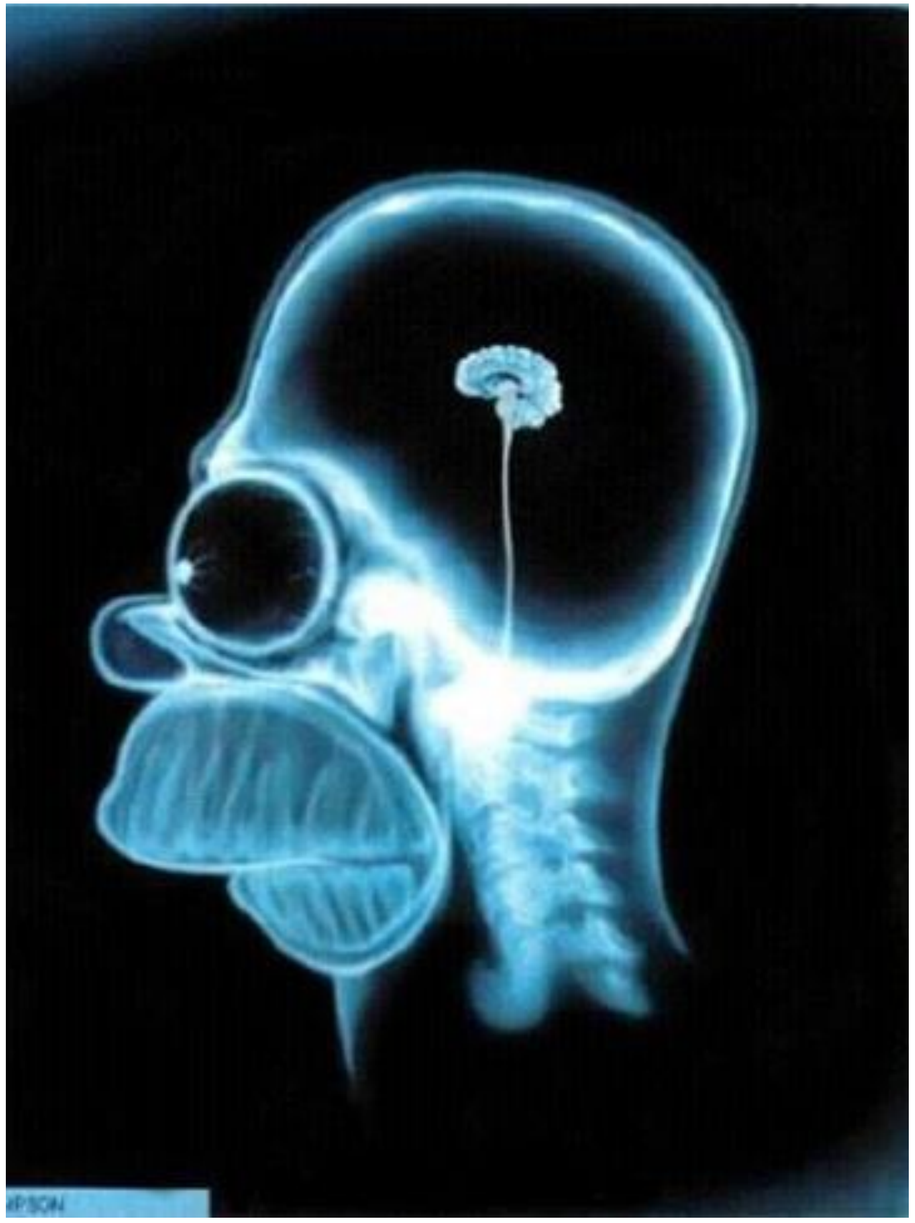
localhost, allora può "fidarsi".

Questa logica ha radici antiche nell'architettura dei sistemi Unix e nei modelli di sicurezza perimetrale, ma nel contesto del browser moderno è ***semplicemente sbagliata***.


ADD COMMA'S TO YOUR PASSWORDS
TO MESS WITH THE CSV FILE THEY WILL
BE DUMPED INTO AFTER BEING BREACHED
UNTIL NEXT TIME
imgflip.com



OpenClaw: un incubo di sicurezza che riscrive le regole dell'IA agentica



Kali GPT Home Features Pricing Blog Contact English

Command-Line Assistance (Bash & ZSH)

Kali GPT can run as a CLI assistant that listens to your terminal input and provides:

- Real-time explanations of commands (e.g., tcpdump, iptables, awk)
- Suggestions for syntax corrections or alternatives
- Advice on common tool options and flags

✅ Example:
You type nmap -sS 192.168.0.1
Kali GPT responds: “You're performing a SYN scan. Want to add OS detection?”

Automated Pentesting Workflow Support

Kali GPT can assist in building or modifying bash scripts for:

- Automated recon & scanning
- Reporting templates in Markdown or HTML
- Log parsing with grep, sed, jq, etc.

It’s like having an AI co-pilot while building your pentesting pipeline.

Tool-Specific Intelligence

Nmap

Scan customization, service detection

Metasploit

Module selection, payload options, post-exploitation tips

Burp Suite

Proxy, repeater, scanner integration

Aircrack-ng

Wireless network attacks & WEP/WPA strategies

Hydra & Hashcat

Brute-force and password recovery tuning

Smart CyberLab

PERCHÉ E COME NASCE SMARTCYBERLAB

PORTARE LA FORMAZIONE PRATICA DIRETTAMENTE NELLE SCUOLE

PERCHÉ LA DIDATTICA IMMERSIVA FUNZIONA: LEARNING BY DOING

globsit

didacta italia

11-13 MARZO 2026
FORTEZZA DA BASSO
FIRENZE

Smart CyberLab

COMPOSIZIONE DEL RACK

COSA SI PUÒ FARE CON IL RACK COMPLETO

globsit

didacta italia

11-13 MARZO 2026
FORTEZZA DA BASSO
FIRENZE

Smart CyberLab

IL PORTALE di Partner
Community SMART CYBER LAB

LEZIONI SEMPRE IN AGGIORNAMENTO CON WEBINAR ED ESERCITAZIONI

Supporto continuo e diretto
Community che promuove la sottocultura hacker
[ethical]

globsit

didacta italia 11-13 MARZO 2026
FORTEZZA DA BASSO
FIRENZE

Smart CyberLab by globsit

Search...

Pietro Alberio

Pagina iniziale | Connettività | Apparati | Academy | News | Eventi & Webinar | Supporto

CONNETTIVITÀ

APPARATI

NEWS

SUPPORTO

Accesso Rapido

Apri ticket

Tutorial

Config. VPN

Webinar

Latest News

Nome	Titolo	Data publicazione
BruteForce Attack	Nuova Lezione	01/03/2026
Man in The Middle Attack	Nuova Lezione	10/03/2026
Sfruttamento della Vulnerabilità EternalBlue	Nuova Lezione	06/01/2026

Smart CyberLab

ARCHITETTURA A CONTAINER E SICUREZZA

Il sistema utilizza container isolati per gestire WireGuard (traffico VPN) e API (gestione peer) su rete interna dedicata.

I container garantiscono modularità, portabilità e scalabilità, permettendo ambienti VPN indipendenti e replicabili.

La separazione dei servizi riduce la superficie di attacco e limita l'impatto di vulnerabilità.

ISOLAMENTO MODULARITÀ SCALABILITÀ SICUREZZA

Smart CyberLab

IL SIMULATORE

SIMULAZIONE LIVE

globsit

didacta italia

11-13 MARZO 2026
FORTEZZA DA BASSO
FIRENZE

Smart CyberLab

DALLA TEORIA ALLA PRATICA E LE NECESSITA' DEL MERCATO

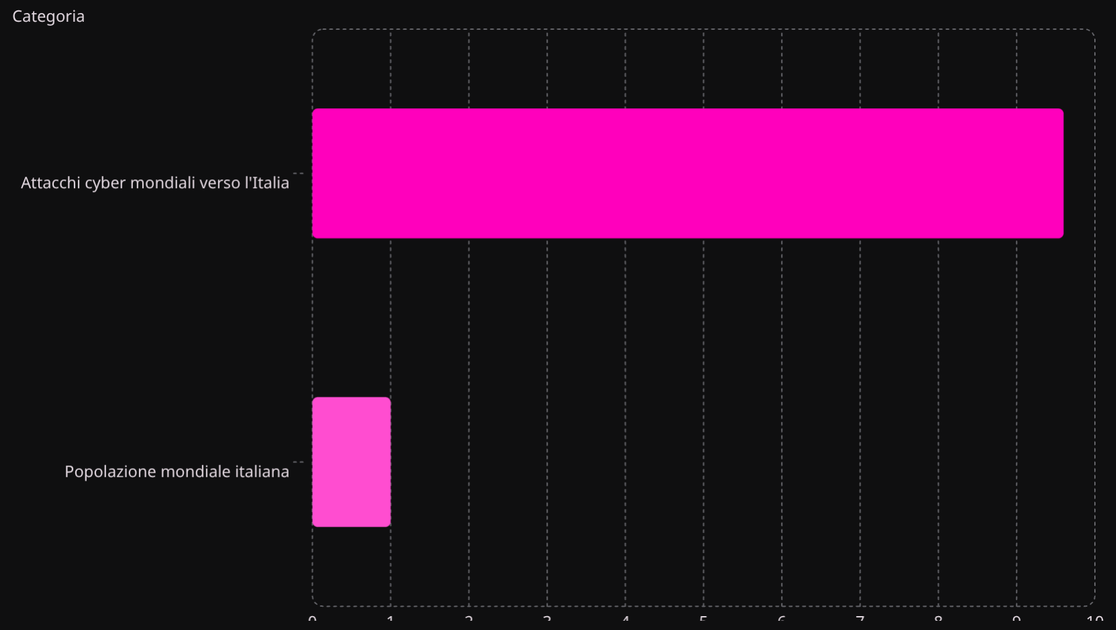
CONCLUSIONI

globsit

didacta italia

11-13 MARZO 2026
FORTEZZA DA BASSO
FIRENZE

L'Anomalia Italiana — 9,6% vs 1%



Una sproporzione allarmante

Nel 2025, l'Italia ha assorbito quasi il **10% degli attacchi cyber mondiali**, pur rappresentando meno dell'1% della popolazione globale. Le organizzazioni italiane sono percepite come vulnerabili e quindi appetibili.

+42%

incidenti cyber in Italia nel 2025

Settori nel Mirino — Manifatturiero e PA

🏭 Manifatturiero

16% degli attacchi manifatturieri mondiali colpisce l'Italia. Le PMI diventano anelli critici nelle supply chain dei settori essenziali, amplificando il rischio sistemico.

🏛️ PA e Difesa

+290% la crescita degli attacchi verso PA e Difesa. Le istituzioni pubbliche sono tornate tra i bersagli principali con escalation significativa.

Il manifatturiero italiano è un'anomalia globale. La vulnerabilità della supply chain trasforma ogni PMI connessa in un potenziale punto di ingresso per attacchi sistemici.

L'Era dell'Inganno — AI e Tecniche d'Attacco

38,5%

DDoS

Tecnica d'attacco principale in Italia: rapida, destabilizzante, a basso costo

+66%

Phishing AI

Crescita delle campagne potenziate dall'Intelligenza Artificiale

L'AI ha abbassato la soglia di accesso al cybercrime, rendendo le campagne di phishing più credibili, personalizzate e scalabili. Il DDoS resta una leva rapida per colpire servizi e infrastrutture.

L'Identità è il Nuovo Perimetro

Il perimetro tradizionale è scomparso

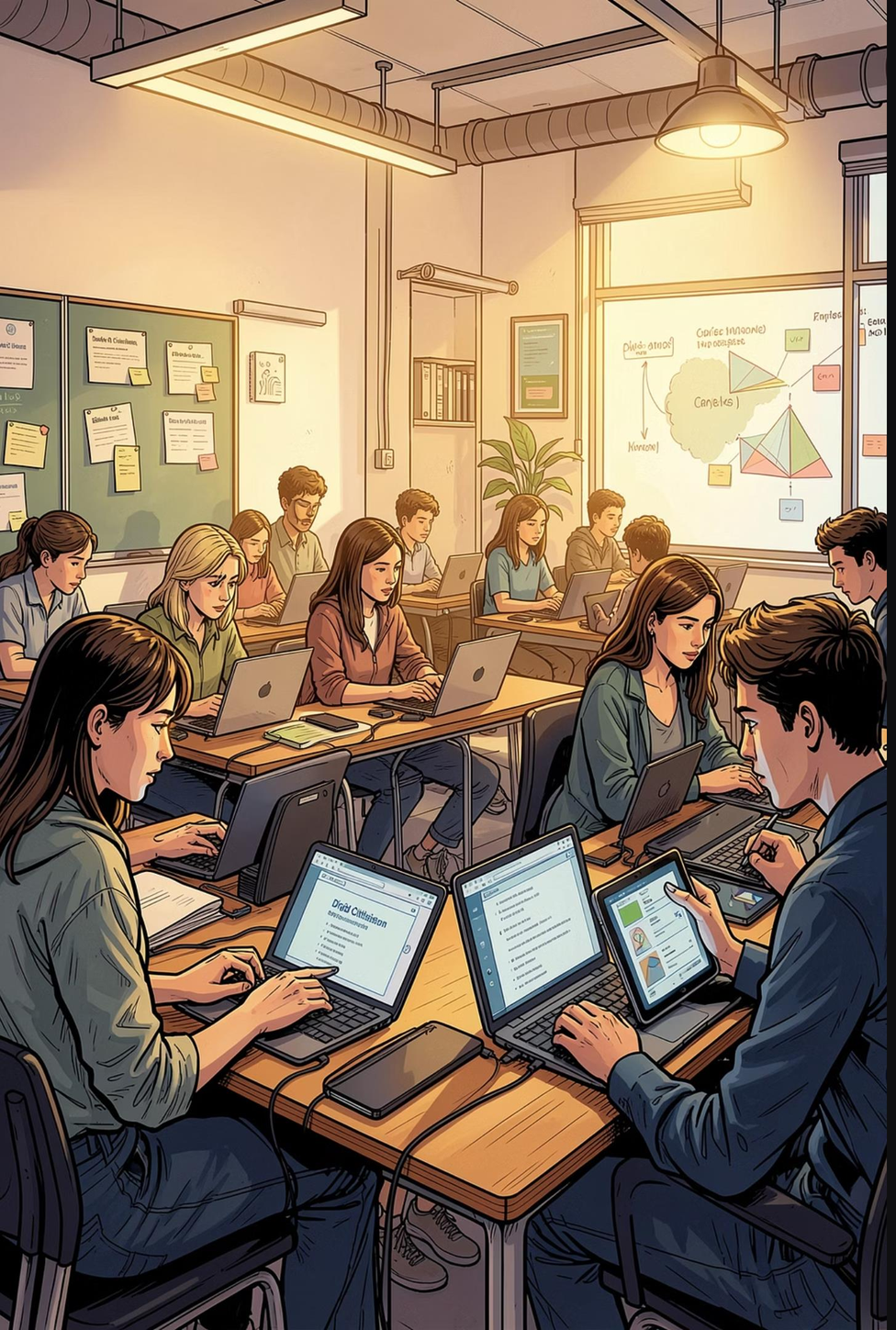
Con cloud, SaaS e lavoro distribuito, la difesa efficace richiede verifiche continue, privilegi minimi e controllo costante degli accessi.

82:1

Rapporto macchine/umani nelle reti aziendali

Log-in, non forzatura

Gli hacker non "forzano" il sistema: fanno log-in con credenziali rubate



Scuola – Educare i "Nodi Attivi" della Difesa

SicuraMente Clusit

Formazione gratuita nelle scuole per trasformare gli studenti da vittime a cittadini digitali consapevoli e attivi.

Moduli Tematici

Intelligenza Artificiale, deepfake, cyberbullismo e phishing: minacce reali che i giovani incontrano ogni giorno.

Resilienza Nazionale

La sicurezza del Paese inizia dalla cultura. Ogni studente formato è un nodo consapevole della difesa digitale collettiva.

Compliance – La Direttiva NIS2

La sicurezza diventa responsabilità del vertice

La NIS2 non è un adempimento burocratico: è una **leva di maturità organizzativa**. La responsabilità sale al Consiglio di Amministrazione e si estende all'intera catena del valore.

→ Governance del rischio

Il board risponde direttamente degli incidenti cyber

→ Supply chain sicura

Un fornitore vulnerabile compromette l'operatività di tutti

Rapporto Clusit 2026

Rapporto Clusit 2026

Il Rapporto inizia con **una panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale (Italia inclusa) nel 2025**, confrontandoli con i dati raccolti negli anni precedenti.

Ci siamo avvalsi anche in questa edizione dei dati relativi agli attacchi in Italia rilevati dal **Security Operations Center (SOC) di FASTWEB + Vodaphone**.

L'analisi degli attacchi in Italia è poi completata dalle **rilevazioni e segnalazioni della Polizia Postale e per la Sicurezza Cibernetica**, che ci hanno fornito dati e informazioni estremamente interessanti su attività ed operazioni svolte nel corso del 2025.

Completa la panoramica di incidenti e attacchi dell'anno scorso, un'analisi degli **Attacchi DDos, ransomware, bot e violazioni delle API in Europa e a livello globale**, realizzata da **Akamay**.

SonicWall transformation.

NEW

TZ 80 lite, 280, 380, 380W, 480, 580, 680, NS*a* 4800, 5800

SonicWall Unified Management

SonicSentry Managed XDR

NEW: MDR/EDR Offerings Expansion

CROWDSTRIKE · Microsoft Defender · Capture Client · CYLANCE · SentinelOne · SOPHOS

NEW: SOHO IoT

New

TZ80

TZ SOHO Series

IoT SOHO Micro SMB

Standard, subscription-based licensing

Sub 1-Gbps Threat Performance

SONICWALL + cysurance

ZTNA Integration in Firewall OS

SOC Expansion EMEA

SONICWALL + BANYAN SECURITY

SONICWALL + SOLUTIONS GRANTED

SONICWALL + TRAPMINE

NEW: Managed Protection Security Suite (MPSS)

NSM 3.0

SonicWall Unified Management

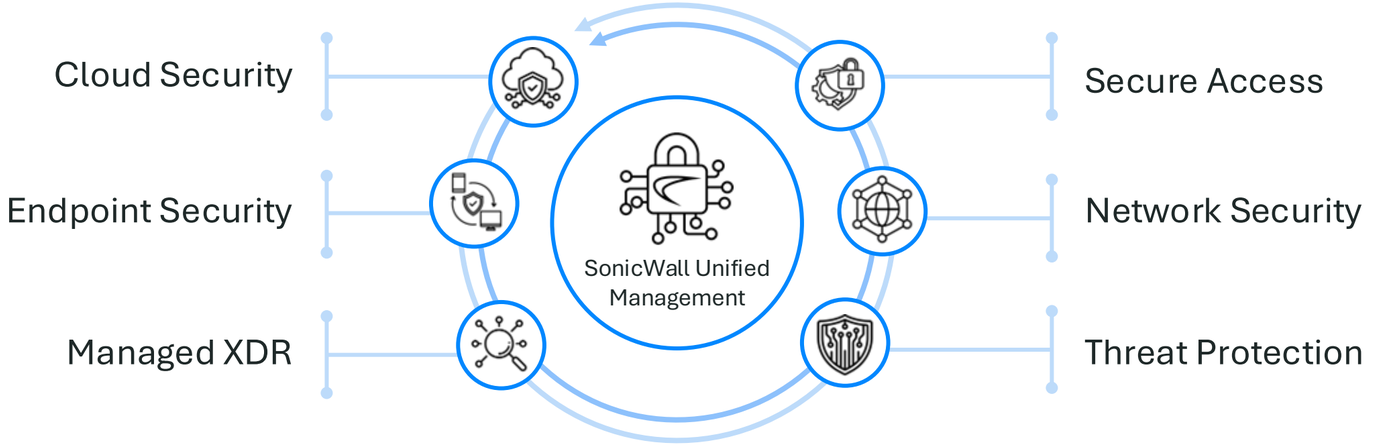
ZTNA / SASE

Managed detection and response

2024 2025

SECURE • SCALABLE • SMART

End-to-end solution suite.



Cyber Warranty

Select Use Cases

- Secure SD-Branch
- Network Segmentation
- Zero Trust Network Security / SSE
- Secure SD-WAN
- Office 365 Security
- SaaS Security
- Secure Wi-Fi

SECURE • SCALABLE • SMART

Modern VPN and Cloud Security.

Manageability

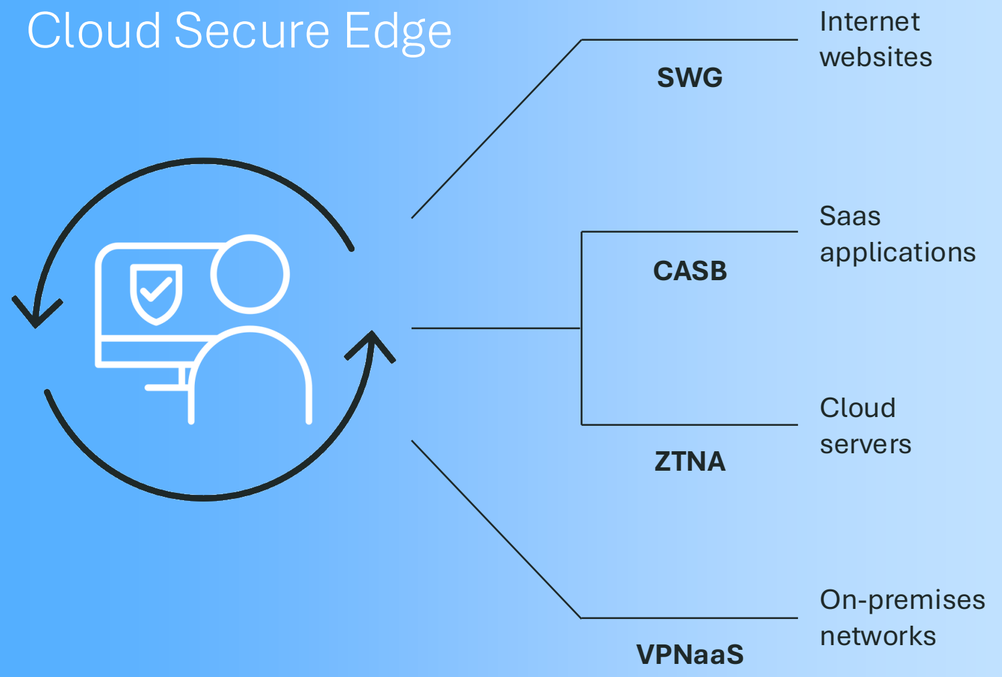
- Easy to manage hardware and network policies
- Easy to Maintain (Monthly patch management needed to manage today's risk)

Security

- Prevents lateral movement
- Constantly evaluates device trust (endpoint security, device, identity, etc.)

Usability

- Reliable user experience

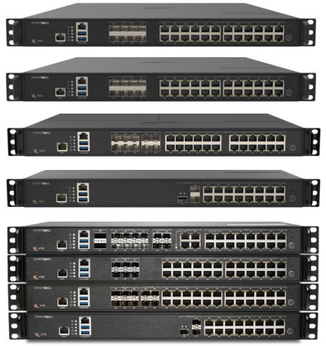


Network security portfolio additions.

NSV

NUTANIX vmware KVM amazon web services Microsoft Hyper-V

NEW
TZ 80 lite, 280, 380, 380W, 480, 580, 680



NEW
NS*a* 4800, 5800

NEW

NSv Series	TZ80 – SOHO Series	TZ Series (entry-level)	NS*a* Series	NSsp Series	Cloud Secure Edge
Private/Public Cloud	IoT, SOHO, Micro SMB	IoT, Micro SMB, SMB/ Branch	Mid Enterprise/Branch	Distributed Enterprises/ Standalone Data Center/ Enterprise	SMB/Enterprise
FIPS, Marketplace/ New RTM	Standard, subscription-based licensing	Standard, PoE, FIPS, Embedded Wireless*	Standard, 1 RU, FIPS	Standard, 1/2 RU, FIPS. High port density, 25G/40G/100G SFP, FIPS	Cloud-delivered Firewall/Zero Trust Access
1 – 8 Gbps Threat Performance	Sub 1-Gbps Threat Performance	1 – 4 Gbps Threat Performance	5 – 30 Gbps Threat Performance	50 – 80 Gbps Threat Performance	Available via Global PoPs

Secure Connect | Lite NEW

Advanced Protection Security Suite (APSS) | Managed Protection Security Suite (MPSS) NEW

cysurance Industry's only embedded cyber warranty included with every firewall

Global Threat Intelligence | Unified Management, Reporting & Analytics | Consistent Experience NEW

THREAT LANDSCAPE

The avoidable risks of an unmanaged firewall.

- Gartner estimates that as much as **60% of breaches** are due to misconfiguration.
- The rate in which **patch management case load** is growing is overwhelming most partners and customers.
- 61% of the time, hackers are **exploiting vulnerable code within days** of it being identified.
- Customers and Partners tend to update vulnerable OS **60-150 days after it is made available** (Infosec Institute).

SECURE • SCALABLE • SMART

Defense across the attack surface.

SonicSentry Managed XDR

Alert Management · Threat Hunting · Threat Mitigation · Log Retention · Reporting

MDR for Endpoint

Protection and response for endpoints

CROWDSTRIKE

Capture Client

SentinelOne

Microsoft Defender

CYLANCE

SOPHOS

MDR for Cloud

Protection and response for cloud apps and email

Cloud Email Security

Microsoft 365

Google Workspace

Cloud Threat Analytics

slack

Dropbox

salesforce

MDR for Network

Any network device from any maker

SECURE • SCALABLE • SMART

The new SonicWall.

- Transformed from leading firewall company to broad cybersecurity solutions provider
- Fastest growing segments are cloud security / ZTNA & managed security services
- SonicWall Unified Management provides consolidated console / management across solutions
- Delivering managed services through dedicated SonicSentry Business Unit
- Firewalls fully managed by SonicSentry team through Managed Protection Security Suite
- Solutions backed by cyber warranties up to $1,000,000
- The platform of choice for MSPs and MSSPs

SONICWALL

NEVER ALONE. RELENTLESS SECUIRITY.

We are SonicWall.

Higher Education

1,500+
of major universities

7.5 million
students

Government

10
defense agencies

1M+
troops

K-12

Thousands
of schools

Millions
students and faculty

Retail

100+
household names

Thousands
distributed locations

THANK YOU

Never alone.
Relentless security.

SONICWALL®

CYBER RESILIENCE ACT

… requisiti di cyber security dei prodotti con elementi digitali