< Deepfake-as-a-Service >|

THREAT INTELLIGENCE REPORT

FACE THE UNPREDICTABLE

FOREWORD

"Dial D for Deepfake" – Will Cybercrime be almost perfect in 2025?

"Dial D for Deepfake". This could have been the title of an Hitchcock thriller, where digital manipulation becomes the ultimate weapon in the pursuit of the perfect cybercrime.

While all forecasts for 2025 suggest that phishing and ransomware will remain the most widespread forms of cyberattacks, artificial intelligence—while enhancing our capabilities in many sectors (healthcare, education, etc.)—is also transforming the cybersecurity landscape. **The creation of synthetic videos, voices, and identities that are indistinguishable from reality now poses an unprecedented threat:** every individual can become a target, every organisation a battleground.

Far from being limited to disinformation, deepfakes are poised to become a key tool in cyberattacks of unprecedented scale. The example of a deepfake attack targeting an entire company's leadership is proof: it's no longer just about swaying public opinion, but about impersonating identities, exploiting trust, and manipulating critical decisions in real time. After "Ransomware" and "Phishing" as-a-Service, 2025 may see the rise of Deepfake-as-a-Service.

Mass industrialization of deception: in this exclusive report, **our Threat Intelligence team investigated Haotian AI,** a company offering face-modification software via Telegram. Some of its promotional messages appear to directly target "Pig Butchering" scams—a long-term psychological manipulation tactic designed to extract money from victims—**highlighting just how industrialized cybercriminal groups have become,** forming full-fledged enterprises dedicated to large-scale fraud and identity theft.

Haotian AI offers easy-to-use, **customizable deepfake software capable of real-time face swaps with disturbingly high quality.** Simple face changes are no longer enough. Today's Pig Butchering scams rely on deepfakes so sophisticated that they're nearly undetectable to the average person.

This report explores the evolution of the threat: **from CEO fraud to banking scams, targeted cyberattacks to geopolitical manipulation, AI is lowering technical barriers and amplifying the impact of these attacks.** In the face of this escalation, the response cannot be purely technological. Advanced detection, multi-factor verification, stronger authentication, collective resilience –the answer must be global and coordinated.

In a world where AI blurs the lines between real and fake, the question is no longer whether we can trust what we see and hear– but whether we're prepared to defend ourselves against **a cybercrime that's becoming almost... perfect.**

At your service,
TEHTRIS team

1.

When AI Protects... and Attacks: The New Cyber Challenge

1.1 2024 : When AI becomes the ultimate weapon on the cyber battlefield

The year 2024 marked a turning point in cyberattacks, which grew more sophisticated, driven by advances in artificial intelligence. Not only have these attacks become more advanced, but they've also increased in volume and become more accessible to criminals. Today, even low-skilled actors can leverage these technologies to carry out large-scale attacks.

Several factors explain this acceleration, including:

- **More mature technology:** Deep learning tools and models are now accessible to the general public, including criminal groups with little technical expertise, who can easily exploit these advanced frameworks.
- **Low-cost "turnkey" solutions:** The rise of pre-trained AI models and freely available APIs makes it easier to automate cyberattacks, eliminating the need for major investments.
- **Highly profitable attacks:** AI-powered attacks—like deepfakes and voice synthesis—are more convincing and harder to detect, increasing the success rate for cybercriminals while minimizing their effort.

Plusieurs campagnes récentes illustrent l'ampleur et la sophistication de ces nouvelles menaces :

> Identity theft via Video Conferencing

Thanks to high-fidelity video deepfakes, **hackers impersonate CEOs or CFOs** during video calls.

*2023: **A Hong Kong company loses $25 million.** The cause? An employee was tricked by a deepfake, convinced he was receiving instructions from his superior... when in reality, he was speaking to an AI-generated imitation.*

> Romance Scams – "Pig Butchering"

Fraudsters use **advanced AI models to generate realistic voices and videos,** allowing them to pose as romantic partners online. AI generates convincing conversations, with bots capable of interacting fluidly for weeks at a time.

*The most widely publicized case remains that of a French victim who, believing she was in a relationship with Brad Pitt, was manipulated **for over a year** by an individual using advanced techniques—specifically AI-generated images and videos.*
*In total, the victim transferred nearly **€830,000 to the scammer,** believing she was helping fund medical treatments for the supposed actor.*

> Fake KYC (Know Your Customer)

Online identity verification processes are increasingly being bypassed using AI. Through real-time simulations of faces and voices, cybercriminals can successfully complete video authentications that are meant to confirm a user's identity.

*In 2024, **several banks and cryptocurrency platforms** reported attacks in which hackers used deepfakes **to open fraudulent bank accounts and launder millions of dollars.***

Whereas in the past, a phone call or video conference **served as nearly indisputable proof of authenticity,** today, an attacker can produce forgeries with unsettling credibility.

1.2 The Cybersecurity challenge: Detecting the Invisible

AI-powered attacks are entering a new dimension, **disrupting the traditional "chain of trust" that once helped distinguish real from fake.** Where a phone call or video conference once served as near-undeniable proof of authenticity, attackers can now generate disturbingly credible forgeries—be it images, voices, or videos—breaking through both psychological and, at times, technical defenses of users.

24/7 - Around-the-clock operations at low cost

Beyond their sophistication, **AI drastically reduces the cost of executing an attack.** Where a criminal campaign once required time and human resources, it can now be fully automated at scale.
Advanced bots can simulate hundreds of simultaneous conversations using elaborate scripts that adapt to each victim—operating continuously, without fatigue or inconsistency.

1.3. Who benefits from the crime? The new players fueling the criminal AI black market

Behind the rise of AI-enhanced cyberattacks lies an emerging underground market.
Technical skills are no longer required—any cybercriminal can now access sophisticated tools through Telegram or even "official" websites **offering solutions such as:**

- **Real-time face-swapping,** allowing identity impersonation during a video call, for example on Zoom or Skype.
- **Ultra-realistic voice synthesis,** capable of imitating a voice with uncanny accuracy, making phone scams much easier.
- **Automated Chat,** with advanced bots that maintain fluid conversations over several weeks—commonly used in pig butchering scams and phishing attacks.
- **Image generation,** enabling the creation of undetectable fake profiles to manipulate targeted victims, often on social media.

In this digital jungle where anonymity reigns,
one name in particular caught the attention of our
Threat Intelligence team at TEHTRIS:
Haotian AI.

This organization alone embodies
the rise of a true underground industry,
where artificial intelligence has become the ultimate weapon for cybercriminals.

2.

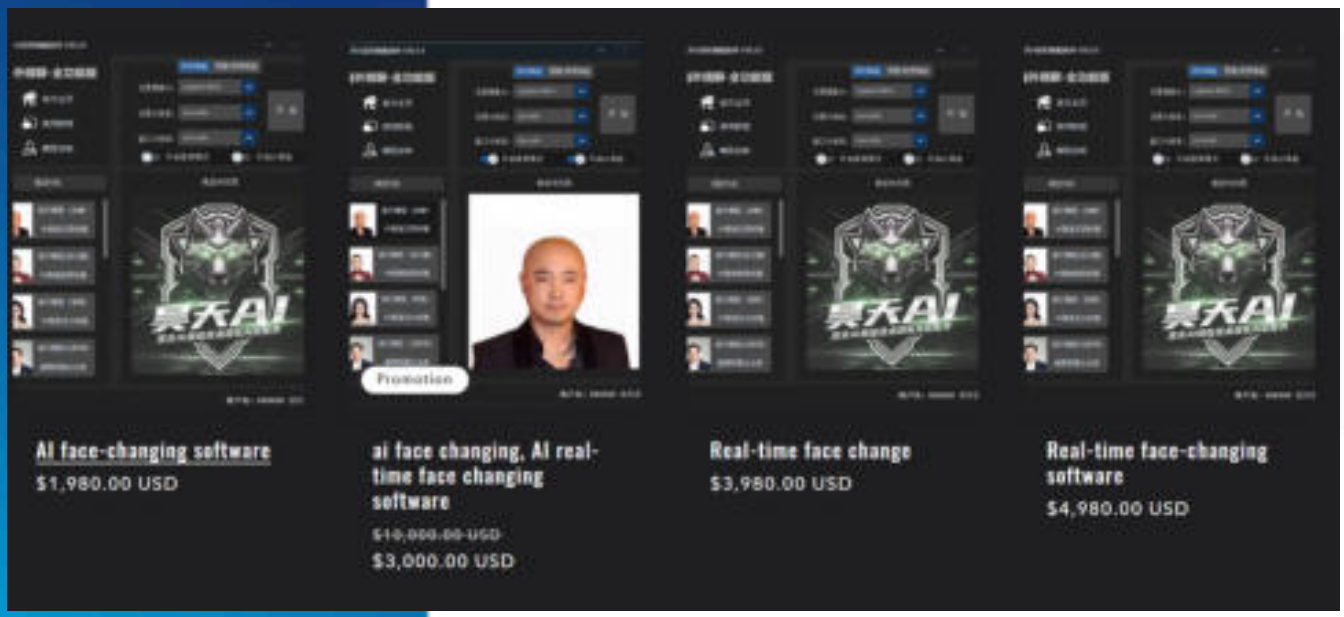
Case Study: Haotian AI

AI Model reseller or a "Deepfake-as-a-Service" example fueling scams?

Promotion pour la solution Deepfake d'Haotian.AI

About Haotian AI

- **A main website: haotian.ai,** active since late 2024 – early 2025.
- **A claimed 20 years of AI R&D experience (an unverifiable info).**
- **A turnkey Deepfake-as-a-Service offering,** including real-time face-swapping software, voice cloning, and automated conversation tools for platforms like Facebook, Telegram, and WhatsApp.



Liste des prix d'Haotian.AI pour du Face swaping en temps réel

2.1 Who is Haotian AI?

Based in Asia, Haotian AI describes itself as an artificial intelligence company headquartered in Phnom Penh, Cambodia.

But behind this technological façade, **it appears that Haotian AI has built a true business model around digital fraud.**

Our OSINT research reveals **multiple indicators suggesting that the company doesn't just sell AI tools—it actively facilitates their use by cybercriminals.**

A company **that embodies the industrialization of deepfakes** in the service of scams?!

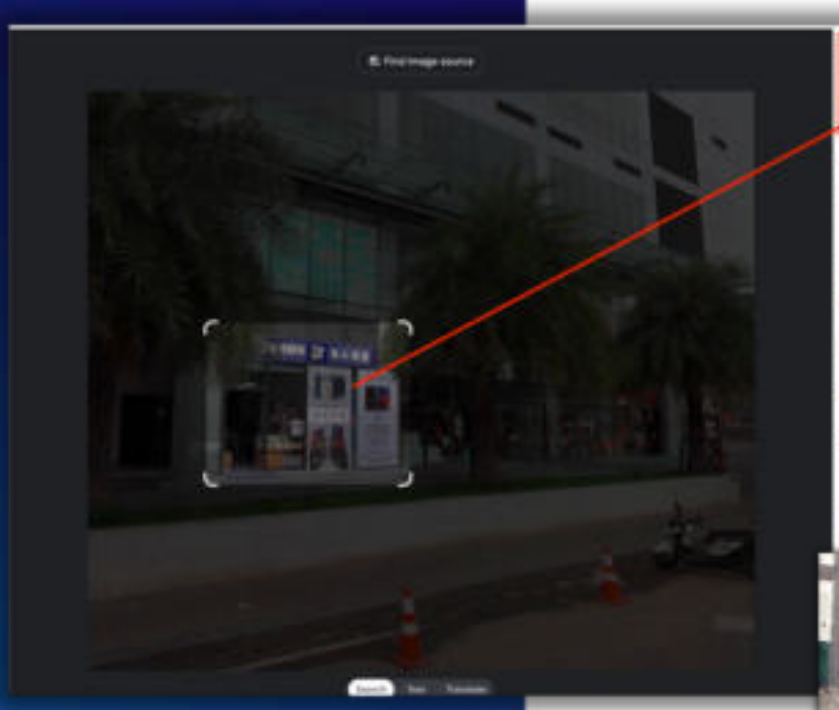
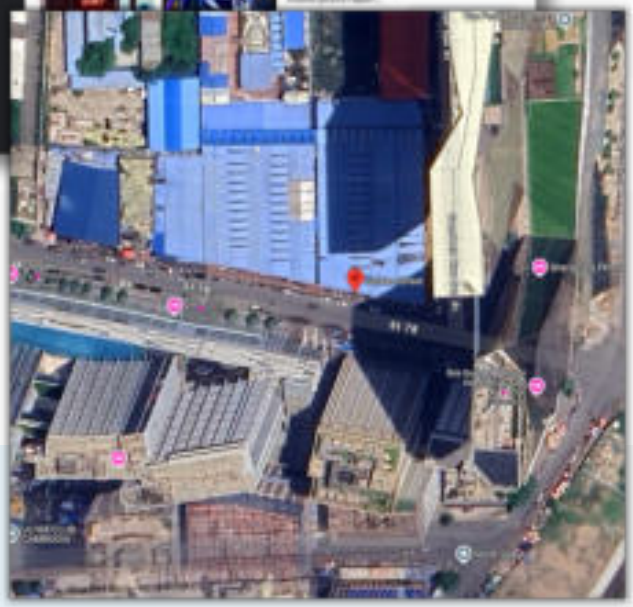


Photo of Haotian AI's storefront



Google Maps view of the Haotian AI store

Chapters 2, 3 et 4 dive into the core of Haotian.AI's business model—an example of "Deepfake-as-a-Service."
Products, marketing, pricing, as well as payment methods, content publishing, and promotion: uncover what lies behind this company that claims to sell AI.

How can we protect ourselves?

Find defensive measures and **recommendations for CISOs and SOC/MDR teams in Chapter 5.**

Behind Haotian.AI lies much more than just a showcase website. This section sheds light on the digital ecosystem surrounding the organization: associated domain names, linked brands, Telegram channels, and parallel networks.

From promotion and customer support to financial transactions, these platforms play a key role in the operation of this "Deepfake-as-a-Service" model.

2.1.1. Domains Used by Haotian AI

Over the months, Haotian AI has used several domain names, such as:

- **haotian.ai** (main site, hosted via Cloudflare, IP registered with Vultr)
- **haotianai.com** (a previous domain, now redirected or inactive)
- **haotianai.us** (another redirection or short-lived usage)

These domain names share several common traits:

- **WHOIS** records containing overlapping details (name, email)
- **Registry entries** that occasionally reference the name “wuyilong” (suspected to be one of the owners or associates)
- The use of the email **ht99532057@gmail.com** for official contact purposes

2.1.2. Behind Haotian.AI: a Telegram network powering the business

Haotian AI appears to be more than just a showcase website:

- An official Telegram channel: **@haotianai**
- Multiple satellite groups (e.g., **@jingliao_ai, @htaihl2851, @haotianai_kf, etc.**) used for customer relations and promotional activities
- Identified “resellers” or “salespersons” **on Telegram**, such as user **@haotianai7** (formerly @Richme77), who advertise in various public or semi-private groups

These Telegram groups appear to serve as central hubs for:

- **Product demonstrations**, including video clips and tutorials on live face-swapping
- **Financial transactions**, often conducted through questionable “escrow” services
- **Customer feedback**, including software installation help, technical issues, and troubleshooting

2.1.3. Other Associated Brands? FaceWap AI

Haotian AI also appears to be linked to a "twin sister" brand: FaceWap AI.

- The same type of products (deepfakes, face-swapping),
- Promotion on Telegram via the group @facewap,
- Use of the same financial services (HuiOne Guarantee).

This dual branding suggests a diversification strategy: the FaceWap AI brand may be targeting a different audience or aiming to bypass potential domain or account suspensions.

2.2. Financial structures: HuiOne Guarantee and Cryptocurrency Laundering

A key element uncovered in the investigation into Haotian AI is its use of HuiOne Guarantee (or "汇旺担保"). On paper, HuiOne Guarantee presents itself as a so-called escrow service:

- The customer deposits funds (often in USDT-TRC20)
- HuiOne holds the funds until the transaction is completed
- The seller (in this case, Haotian AI) receives the money once the customer confirms successful delivery of the product or service

2.2.1. The real role of HuiOne Guarantee

In practice, HuiOne Guarantee functions more like a money laundering system or "gray bank":

1. **Anonymization:** Multiple USDT addresses are created, then disappear or rotate with each sale
2. **Lack of verification:** No strong KYC process; most transactions are "approved" as soon as the buyer and seller agree
3. **Fragmentation:** Large sums are often broken down into smaller transactions (e.g., split into multiple transfers of 200 or 500 USDT)

Payment Confirmation

Telegram groups such as @htaihl2851 or @zqaihl792 (identified as "HuiOne Guarantee groups") contain recurring messages like:
[Date / Amount / Buyer Username] transferred [xxx USDT] to [xxx wallet] – Transaction completed.

These payment confirmations appear dozens of times, pointing to a significant volume of transactions tied to Haotian AI or FaceWap AI products.

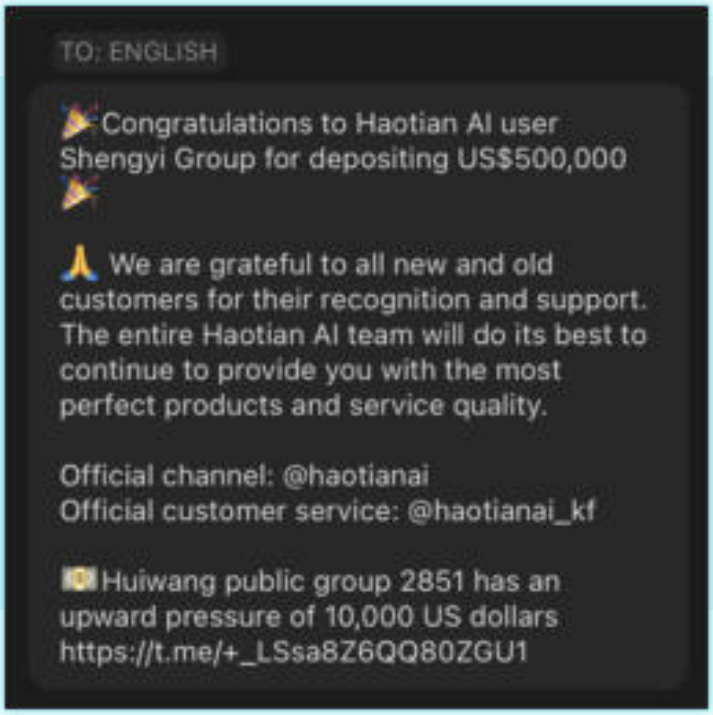
Proof of Crypto Transactions

Evidence of cryptocurrency transactions

2.2.2. Traced cryptocurrency addresses

Haotian AI and FaceWap AI have used multiple USDT-TRC20 addresses.
The following are illustrative examples:

- **TRrAhAkLvAF7RiMQoJMLjHq51u9Q1ohU7D**
- **TBWLu9ijf6ojuoVRRRS6HpjKZuNmDDDDDD**
- **TWticPHWiByHDQpwDKLbofNrNxoj666666**
- **TUsPdGKmYzcQM1YEKoz9cVvQF88haotian**
- **TR3b1hxsDdumqUmmPXHP1wvkhLh4FFFFFF**



More detailed analyses (via Tronscan, for example) show that these wallets receive deposits –often ranging from 200 to 9,000 USDT– and then quickly transfer the funds to other addresses, making final traceability significantly more difficult.

2.3. Behind the scenes of Haotian AI: WHOIS Data and potential identity

2.3.1. A recurring identity in the investigation: "Wu Yilong" (wuyilong22@gmail.com)

Several data leaks in China mention an individual named "Wu Yilong" (吴义龙), whose personal information (ID, phone number, etc.) points to the Anhui province.

The email mislead@163.com is also associated with him.

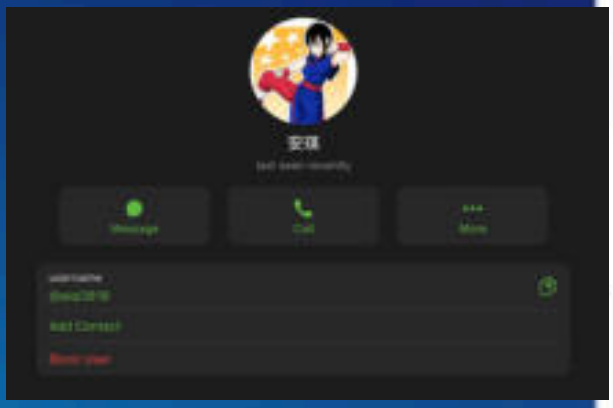
In the WHOIS records of "haotianai.com" and "haotianai.us", the email "wuyilong22@gmail.com" appears.

This suggests that someone named Wu Yilong may be the owner or a member of the leadership team behind Haotian AI.

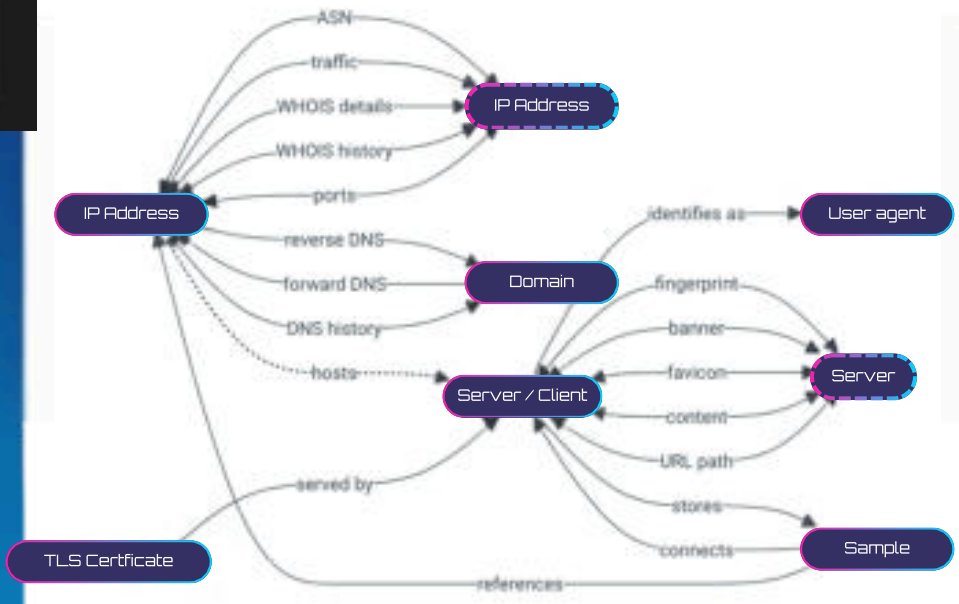
2.3.2. Cross-linked Telegram Accounts and Phones

On the mindmaps we provide (see image), we highlight +855 phone numbers (Cambodia) linked to Telegram accounts listed as administrators or "bosses" of Haotian AI.

+85599532057 (lié à l'email ht99532057@gmail.com).
+855966926960 (compte @htai_df avec logo Haotian).
+855968594588 (autre contact suggéré dans des vidéos promotionnelles).



The investigation suggests the existence of a core group operating out of Cambodia, potentially with connections in China or Southeast Asia.



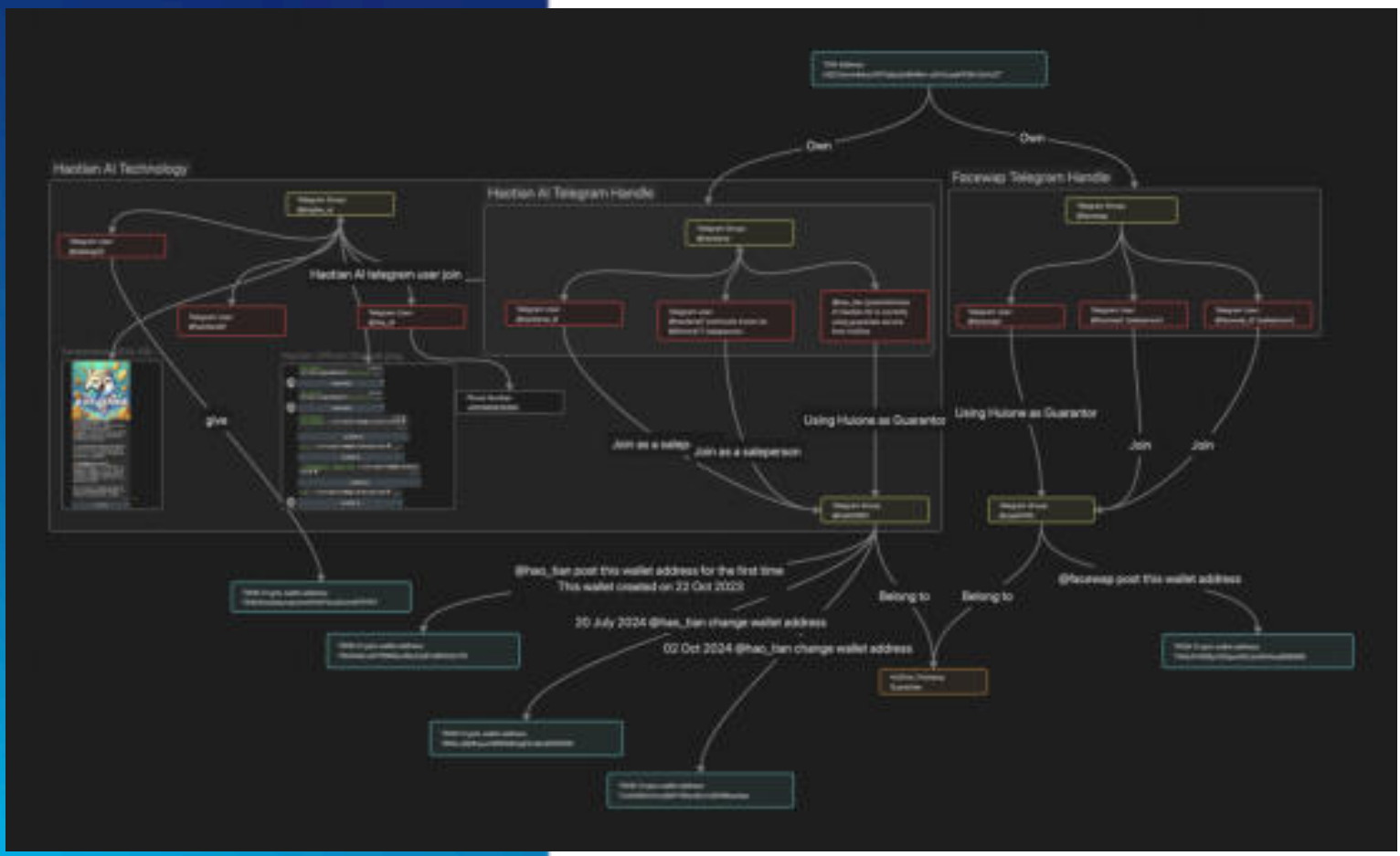
The Haotian AI Ecosystem

This mindmap provides an overview of the Haotian AI ecosystem and its connections, particularly with Facewap AI. It highlights the following:

1. **Haotian AI and its users:**
   - Presence of Telegram accounts (e.g., @haotianai6) linked to the official channel
   - Discussion groups where announcements and advertisements are actively shared
2. **Roles and identities:**
   - Sales representatives or points of contact (e.g., @haotianai7) acting as intermediaries
   - A Cambodian phone number (+855) associated with one of the profiles
3. **Financial and crypto services:**
   - Use of TRON addresses (USDT, TRC20) for transactions
   - Frequent wallet changes (e.g., "20 July 2024 change of wallet address")
4. **HuiOne Guarantee (Escrow) :**
   - Service used by Haotian AI and Facewap AI to anonymize crypto payments
5. **Facewap AI, a parallel entity:**
   - Related structure, sharing the same channels and intermediaries.
6. **Blockchain Variety:**
   - Mention of a TON address, indicating multiple financial pathways.

Analysis and relevance:

- Each node represents an actor (individual, crypto wallet, Telegram group)
- Arrows indicate the links between services, transactions, and address changes
- This map helps visualize an organized network intertwining AI, deepfakes, and anonymized payments



3.

AI at the heart of large-scale fraud: Deepfakes, voice cloning, and automated Bots

3.1. GANs: The Foundation of Haotian AI's Deepfake

Haotian AI makes practical use of Generative Adversarial Networks (GANs) in various ways, including:

- **Real-time face-swapping:** Overlaying a "target" face onto an operator's during a video call (Zoom, Teams, WhatsApp)
- **Fake face generation:** Creating convincing fictional profiles for social media (LinkedIn, Facebook) or fake testimonials

Les GANs - Ultra-realistic image generators

- **Haotian AI's deepfakes primarily rely on techniques derived from GANs** (Generative Adversarial Networks).
- **A generator algorithm** attempts to create a realistic image (or video), while **a discriminator** tries to detect whether it is fake.
- Through repeated iterations, **these models eventually produce near-perfectly realistic results**, capable of deceiving both humans and even some detection algorithms.

3.2. Voice Synthesis: Voice cloning and bypassing KYC verification

Banks and fintech platforms are increasingly implementing voice-based identity verification (e.g., "Hello, please state your name and date of birth").
In response, Haotian AI offers a "Deep Voice" module—a sophisticated voice cloning tool designed to bypass these verification systems.

Features of the Deep Voice module:

- **Highly accurate imitation,** replicating the accent, intonation, and rhythm of a target voice
- **Live demonstrations on Telegram,** where operators use AI to speak in someone else's voice in real time

Use Cases:

- **Phone scams,** impersonating a manager or relative to request urgent wire transfers
- **Identity theft in KYC procedures,** generating a voice that matches a stolen audio sample to pass voice-based authentication systems

"**The victim is the prey** – carefully 'fattened up' over time – **before being financially 'slaughtered'.**"

3.3. AI to the tervice of romance scams: The "Pig Butchering Machine"

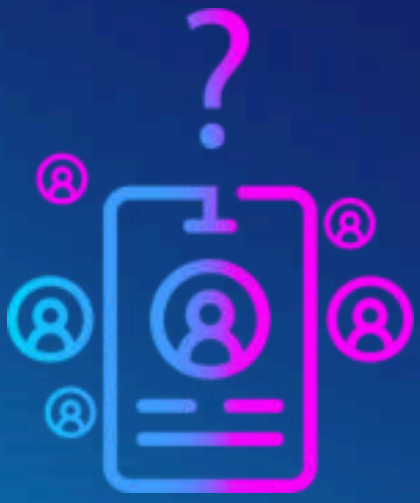
3.3.1. the concept of "Pig Butchering"

TTPs (Tactics, Techniques, and Procedures) of Pig Butchering Scams:

- **Emotion-driven manipulation:** The victim is the "pig," gradually "fattened up" emotionally over time before being financially "butchered"
- Criminals spend **weeks or months building a relationship**–romantic, friendly, or posing as a crypto mentor
- Once trust is established, they begin **pressuring the victim to invest or send increasing amounts of money**
- When full confidence is gained, the scammer **vanishes with the funds**

3.3.2. AI-Driven automation: a new level of scam efficiency

In a mindmap, we reveal how Haotian AI has industrialized romance scams using **multichannel chatbots designed to manipulate hundreds of victims simultaneously.**



Social Engineering Bot Capabilities:

- **Advanced NLP Interaction:** The bot understands and generates natural, engaging responses in real-time
- **Multiple Identity Management:** A single bot can simulate dozens–or even thousands–of profiles simultaneously
- **Scripted Manipulation Scenarios:** Conversations follow evolving scripts, with phases of flirtation, emotional persuasion, and fake investment proposals
- **Deepfakes as Reinforcement:** The bot can send fake images and videos to "prove" a male or female identity, boosting credibility

The combination of voice cloning, video deepfakes, and conversational bots allows scammers to **eliminate human effort.**
They no longer need to recruit operators to maintain long-term interactions with victims.

AI operates around the clock, making these scams more massive, more lucrative, and significantly harder to detect.

4.

Exploring the mindmaps: Bot architecture, money laundering, and victim engagement

Beyond general descriptions, we dive deeper into the mindmaps (heuristic maps) reconstructed from archives, Telegram groups, and screenshots. From these, several key analytical "blocks" emerge:

4.1. Architecture of Automated Bots

TEHTRIS mindmaps reveal a recurring structure:

1. **Data Collection Module (Social Mining):**
   - Gathers profile information (age, location, interests) via platforms like Facebook, LinkedIn, etc.
   - Compiles "contextual cues" to help the bot tailor its approach to each victim
2. **NLP Interaction Module:**
   - Generates responses adapted to the victim's tone and inferred preferences
   - Suggests "pivot conversations" (e.g., "What do you think about crypto?" or "Have you ever invested in trading?")
3. **Social Engineering scripts:**
   - Script #1: Build a friendly relationship
   - Script #2: Introduce an investment opportunity
   - Script #3: Deliver an initial "success" to gain the victim's trust
   - Script #4: Encourage further investment
4. **Multimédia Module:**
   - Integrates photo/video deepfakes to create the illusion of a real person
   - Sends short AI-generated voice notes to reinforce the idea of a physical presence

4.2. Cryptocurrency-based laundering techniques

Blockchain transaction and OSINT analysis:

- **Fund fragmentation:** Large sums (e.g., 5,000 USDT) are often split into 10 smaller transfers of 500 USDT
- **Multiple wallets used:** Each sale results in the creation of a new address
- **Third-party services:** HuiOne Guarantee orchestrates fund movement, formalized through a Telegram "transaction validation" group
- **Smoke screens:** Funds sometimes pass through 2–3 intermediary ("buffer") wallets before reaching the final destination

4.3. Prolonged victim engagement

Another key insight revealed by our mindmaps: victims are continuously engaged over long periods:

1. **Initial Approach Phase:** Compliments, shared interests, daily check-ins
2. **Comfort Phase:** Virtual gifts, scripted video interactions, even fake "video calls" using deepfakes to simulate presence
3. **Turning Point Phase:** Investment proposals, fake profit screenshots, enticing returns
4. **Final Scam Phase:** The victim sends a large sum—sometimes multiple times—under emotional pressure or urgency (e.g., "I have a medical emergency, I really need help…")

The mindmaps also highlight decision indicators used by the bots:

- **How is the victim behaving?**
- **What's their level of trust?**
- **What are their financial limits?**

The chatbot adapts its messaging to keep the hook in and push toward the desired outcome.

4.4. Voice synthesis and KYC evasion

LWhen a victim or institution requests additional verification (e.g., "Send me a voice message to prove you're real!"), Haotian AI leverages voice synthesis modules:

- The attacker simply clicks a pre-configured voice template
- The system plays a short message, such as:
- "Hi, it's me, [name]. Don't worry, I'm just in a meeting right now."

In more advanced scenarios, attackers can even **make live phone calls** using **voice cloning** tools through IP telephony, imitating the target's voice in real time.

4.5. Deeper Immersion: conversation examples and Telegram screenshots

To illustrate the reality of this modus operandi, here are some anonymized examples collected from Haotian AI's Telegram channels:

1. **Promotional message:** "Try our Face Swapping Tool V5.0, real-time version—perfect for 'Zoom conversations'. Special price: 1,280 USDT. On-site installation available in Phnom Penh!"
2. **Transaction confirmation:** "Client [@xxx] deposited 500 USDT via HuiOne Guarantee — Contract #2851 finalized. Software installation in progress…"
3. **Chatbot example:** Screenshots of a chatbot impersonating a young woman, sending deepfake selfies and short AI-generated voice messages, maintaining emotional connection over time.

4.5. Deeper immersion: sample conversations

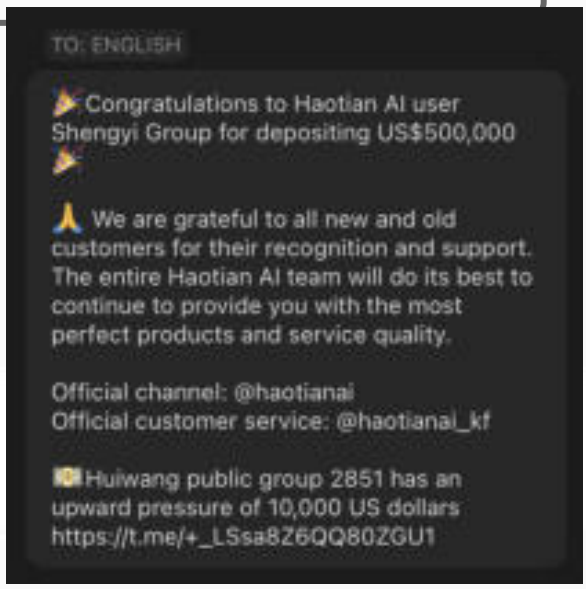
To illustrate the reality of the modus operandi, here are a few anonymized examples collected from Haotian AI's Telegram channels:

1 **Promotional Message:**

"Try our Face Swapping Tool V5.0 – real-time version, perfect for 'Zoom conversations'. Special price: 1,280 USDT. On-site installation available in Phnom Penh!"

2 **Transaction Confirmation:**

"Client [@xxx] has deposited 500 USDT via HuiOne Guarantee – Contract #2851 finalized. Software installation in progress..."



3 **Chatbot :**

The entire conversation is carried out by an AI impersonating a young woman, sending deepfake photos to build trust and emotional connection.

5.

Defensive measures and recommendations for CISOs and SOC/MDR teams

5.1. Hyper-Automated XDR: A Critical Response to Emerging Threats

The rise of AI-powered cyberattacks is radically reshaping detection and response strategies. When it comes to protecting operating environments, traditional solutions—like signature-based antivirus or post-incident EDR—are no longer sufficient against these evolving threats.

Key challenges include: :

- **Identifying deepfakes in video conferences,** which can deceive employees into performing critical actions within their organization's IT systems
- **Detecting automated conversational scripts,** where a bot manipulates an individual over weeks, potentially leading them to unintentionally compromise their company's security

Currently, our analysis show that these techniques are not yet widely used for advanced intrusions. Traditional phishing attacks remain the most dominant form of cyber threat at this stage.

Our current analysis shows that these techniques are not yet widely used for advanced intrusions—traditional phishing attacks still dominate. However, a new wave of threats is on the horizon: cybercriminals may soon move beyond basic phishing emails to long-term manipulation via conversational AI agents, significantly increasing the effectiveness of social engineering.
As social engineering intensifies, leading to attacks initiated from within infrastructures through employee manipulation, cybersecurity must evolve.

Defense in depth must go beyond perimeter protection and adopt proactive solutions that anticipate threats before they materialize.
This is precisely why **we advocate for a hyper-automated XDR approach**—a system designed not only to counter known threats but also **to detect and respond to emerging, AI-driven attacks in real time.**

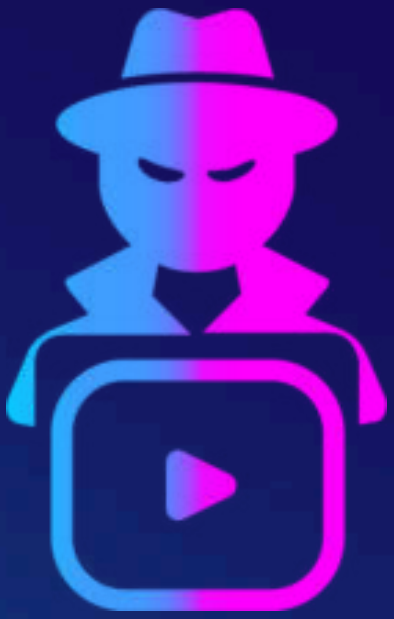
Why TEHTRIS is committed to hyper-automation

TEHTRIS XDR AI

AI and automation have become powerful weapons in the hands of cybercriminals.

The response must include solutions that minimize human intervention, such as:

- **Automatic isolation of endpoints** showing suspicious behavioral anomalies
- **Instant blocking of suspicious IP addresses and domains**, without manual delay
- **Adaptive Machine Learning,** which enhances real-time detection by learning from every new attack attempt



5.2. Behavioral detection and analysis of weak signals

In the face of deepfakes and voice cloning, **traditional detection methods are becoming obsolete, as these attacks often leave no technical signatures that can be easily exploited.** However, certain behavioral anomalies can still be identified, such as:

- **Unusual delays during video calls,** which may indicate real-time deepfake generation
- **Subtle voice inconsistencies,** such as artificial intonations or slightly delayed responses
- **Overuse of urgent communication tactics,** including pressure phrases like "This transfer needs to be completed immediately!"

Employees and users must be trained to spot these weak signals, and companies should establish stricter protocols for sensitive communication channels.

5.3. Monitoring financial flows and Blockchain OSINT

Tracking illicit financial flows is critical for mapping criminal networks. Cryptocurrencies play a key role in financing AI-driven attacks, making blockchain monitoring and OSINT (Open Source Intelligence) more crucial than ever.

Effective methods include:

- **Analyzing public transactions**, to detect recurring patterns and flag suspicious addresses
- **Leveraging OSINT tools,** to automatically extract crypto addresses published on platforms like Telegram and cross-reference them with transaction amounts and dates
- **Cross-company collaboration,** by sharing blacklists of fraudulent addresses, making it easier to freeze malicious funds

The goal is to disrupt the financial infrastructure of cybercriminals before they can launder their profits from scams and online fraud.

5.4. Sensibilisation et Formation des Collaborateurs

Even the most advanced cybersecurity technologies will fail if employees are not trained to recognize AI-driven threats. An active awareness strategy is therefore essential, and should include:

- **Deepfake simulations:** staging fake videos of executives requesting urgent wire transfers, then analyzing employee reactions and learning from them
- **Voice phishing drills:** testing team alertness with AI-generated fraudulent calls
- **Real-life scenarios:** live demonstrations of face-swapping to create a psychological "shock factor" and lasting awareness

Training users is a critical line of defense against these new forms of cyberattacks. **An informed and alert workforce is far more effective than relying on technical defenses alone.**

6.

Industrial and forward-looking impacts: “Cyberfraud 2.0” in 2025

6.1. Toward a new level of industrialization

The infrastructure behind Haotian AI highlights a growing trend: the professionalization of AI-based criminal services.

- Complete packages: Tech + training + money laundering + customer support (via Telegram)
- Economies of scale: A single hub (e.g., Phnom Penh) can provide technology to hundreds of criminal groups worldwide
- Rapid adaptability: Products evolve quickly (V4, V5, etc.), bypassing early detection mechanisms

6.2. Increased Risks for Businesses and Governments

- BEC attacks (Business Email Compromise) enhanced with video and audio—ushering in the era of eBEC (enhanced BEC)
- Industrial espionage: Deepfakes of senior executives could be used to extract sensitive information from engineers or production managers
- Political destabilization: Use of face-swapping to generate fake official statements or falsified public appearances in media

6.3. The importance of international cooperation

Since Haotian AI is based in Cambodia but operates globally, collaboration between agencies like Interpol, Europol, and national law enforcement is essential. This should include:

- Sharing IOCs (Indicators of Compromise) linked to malicious actors (e.g., USDT addresses, IPs, Telegram IDs)
- Leveraging anti-money laundering laws to put pressure on services like HuiOne Guarantee
- Raising awareness among local jurisdictions hosting these operations to encourage intervention (server takedowns, criminal investigations)

CONCLUSION

A major challenge for 2025 and beyond

Haotian AI represents the convergence of several technological trends that are disrupting cybersecurity: hyper-realistic deepfakes powered by GANs, real-time voice synthesis capable of bypassing authentication controls, autonomous conversational bots able to manipulate victims over the long term, and money laundering facilitated by opaque financial services such as HuiOne Guarantee.

These tools, accessible to cybercriminals without advanced technical skills, are making attacks more convincing, more automated, and more profitable. The consequences are already being felt: **massive financial fraud, industrial espionage on an unprecedented scale, large-scale social engineering, and a surge in blackmail and sextortion cases.**

In the face of this rapidly expanding threat, a swift and coordinated response is essential. **CISOs must strengthen cybersecurity policies, integrate deepfake detection capabilities, and raise awareness among their teams about new forms of AI-driven manipulation.**

SOC and MDR teams must adopt advanced threat intelligence tools capable of analyzing weak signals on platforms such as Telegram or the blockchain.

Governments and law enforcement agencies must intensify international cooperation, sanction financial enablers, and accelerate the freezing of assets linked to criminal cyber activity.

The rise of Haotian AI is not an isolated phenomenon, but rather a symptom of a new era of cyberfraud—Cyberfraud 2.0—powered by artificial intelligence.

Unless we adopt a proactive approach, combining behavioral analysis, anti-money laundering strategies, and international collaboration, these attacks will only continue to grow in sophistication and impact.

2025 may well mark the year when cybercrime fully shifts into a new era - one of automated, scalable, and nearly undetectable criminal activity.

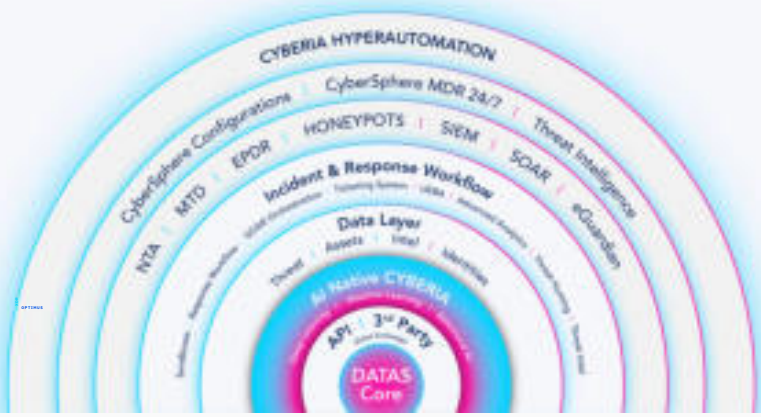
TEHTRIS XDR AI

TEHTRIS SOLUTIONS

TEHTRIS XDR AI PLATFORM

A single console for global orchestration and security

Unify your cybersecurity by bringing together all your solutions in a single console for high-speed detections and responses. Within the TEHTRIS XDR AI PLATFORM, you will find an **EDR**, **MTD**, **SIEM**, **Honeypots**, **NTA**, **CYBERIA**, **Threat Intel**, **Zéro Trust Response**, **Email Protection** and **Identity Access Management**.



Orchestrate all your cybersecurity tools simultaneously, including your existing solutions such as Zscaler and Proofpoint, with the TEHTRIS XDR AI PLATFORM. Our platform is available in our secured cloud or on-prem. Easily deploy it in your ecosystem with in & out APIs. With its customizable playbooks and its hyperautomation capabilities you will get immediate response to cyberattacks.

TEHTRIS SOAR

Orchestrate all your solutions and enable Hyperautomation at the service of your teams

Saving time is essential when remediating attacks. In order to achieve this objective, TEHTRIS has designed its own SOAR. Perfectly integrated into the XDR Platform, our SOAR orchestrates the actions of your cybersecurity tools and automates them. Combined with CYBERIA (artificial intelligence), the detection, contextualization and response to incidents are hyperautomated. Supported in its decision making and freed from repetitive tasks, your SOC gains decisive seconds during cyberattacks. Interoperate your cybersecurity for augmented and hyperautomated remediation.

TEHTRIS SOLUTIONS

THREAT INTELLIGENCE

Our Threat Intelligence for real-time neutralization

Our Threat Intelligence is directly integrated into the TEHTRIS XDR AI PLATFORM, giving you full visibility on all available threats. Our cybersecurity solutions are systematically linked to the TEHTRIS Threat Intelligence. As soon as a cyberattack is attempted, the TEHTRIS Threat Intelligence analyses, (also using our AI CYBERIA), to hyperautomate your responses to attacks for real-time neutralization without human action. You can subscribe to our Threat Intelligence service on its own, or benefit from it automatically if you are a customer of a related TEHTRIS product. The knowledge base consultation is also available via API.

CYBERIA

Enhance your cybersecurity with our artificial intelligence. With CYBERIA, you are protected from threats undetectable by humans.

Addressing the pressing challenges faced by cybersecurity experts, TEHTRIS has invested and developed its proprietary Artificial Intelligence: TEHTRIS CYBERIA, a multi-modular AI and a cornerstone component of TEHTRIS XDR AI PLATFORM. Overcoming cyber security workforce shortage and fatigue, TEHTRIS CYBERIA is embedded through TEHTRIS XDR AI PLATFORM, offering hyperautomation of real-time detection, triage of every single alert, without compromise, remediation, without human intervention VS traditional approaches based on use-cases and filters creating blind spots: a safer alternative to cyber solutions currently offered on the market.

ABOUT TEHTRIS

TEHTRIS, a mission-driven company, has been engaged since 2012 in the fight against cyber espionage and cyber sabotage as a provider of cybersecurity software.

With its «Zero Trust» approach and a unique «Security & Ethics by design» concept, TEHTRIS supports organizations of all sizes and sectors, guiding them to anticipate and confront the unpredictable and become exemplary guardians of their cyber space.

Deployed across the world, the TEHTRIS XDR AI PLATFORM stands out as the ultimate hyper-automated cybersecurity solution. By ensuring real-time detection and neutralization of cyber attacks, ransomware, and malicious behaviors without requiring human intervention, it also guarantees interoperability with market security solutions via its APIs.

Combining active protection from installation with deployment simplicity and continuous support from our experts, it provides users with a holistic view of their infrastructure while preserving the confidentiality of their data 24/7.

By continually enriching its Threat Intel database through globally deployed sensors, TEHTRIS ensures high-level contextual detection and prediction of security alerts, through behavioral analysis and its CYBERIA Artificial Intelligence.

Compliant with all current regulations including GDPR and NIS2, TEHTRIS provides organizations with the confidence needed to address cybersecurity challenges, thus strengthening their defense posture against active and emerging threats.

Follow us on:

LinkedIn Twitter