TEHTRIS
FACE THE UNPREDICTABLE

MADE IN EUROPE

CIBERSEGURIDAD: CARA Y CRUZ DE LA INTELIGENCIA ARTIFICIAL

Tabla de contenidos

1. Un crítico panorama de amenazas mundial 3
2. Soluciones XDR y EDR para detección y respuesta 5
3. MTD: La defensa que el móvil necesita 6
4. Cómo la inteligencia artificial impulsa la seguridad 7
5. Más visibilidad, más protección 9
6. TEHTRIS tiene la respuesta 10

Un crítico panorama de amenazas mundial

Todas las empresas tienen una preocupación en común: garantizar la seguridad cibernética en sus operaciones. No importa su tamaño, sector de actividad o ámbito geográfico en el que se encuentren instaladas. Desde la compañía más modesta hasta aquellas de carácter multinacional y con infraestructuras críticas pueden convertirse en objetivo de unos ciberdelincuentes ya profesionalizados en el contexto digital. Los criminales no discriminan e intentarán diversificar sus esfuerzos para causar el mayor daño posible.

La transformación tecnológica acelerada a la que se han visto sometidos los negocios durante los últimos años complica la situación. **La superficie de ataque se ha expandido.** Cada vez hay más dispositivos conectados y se utilizan servicios basados en la nube, que favorecen la colaboración entre profesionales que trabajan desde casa y en la oficina y que son escalables. Pero estos avances también generan una nueva oportunidad para robar información y lanzar campañas de **espionaje**.

Entre las principales amenazas destaca el ransomware, un tipo de malware que secuestra equipos y es capaz de cifrar los datos contenidos en ellos para entorpecer su uso. El modelo RaaS para alquilar ransomware como servicio ha ganado popularidad, al igual que la exfiltración de archivos para forzar el pago del rescate. La última táctica consiste en amenazar con divulgar el nombre de las víctimas. Los extorsionadores conocen a los proveedores y las cobertura de los ciberseguros, lo que les permite afinar sus acometidas y también sus peticiones.

Detrás de este malware se esconden innumerables actores. En la actualidad existen unos 1.900 grupos diferentes. Lo preocupante, más allá de su cuantía, es que crece la afiliación entre ellos, con la puesta a la venta de herramientas en la dark web y la incorporación de pequeños lobos solitarios a la guerra cibernética, así como la unión de fuerzas entre delincuentes para llevar a cabo sus ofensivas y compartir el botín.

La segunda gran amenaza es la **explotación de vulnerabilidades** de software que no han sido parcheadas. Pero hay más. Ataques DDoS de denegación de servicio que causan tiempos de inoperatividad y que en muchos casos están ligados a la inestabilidad geopolítica y el hacktivismo, las suplantaciones de identidad de individuos y marcas conocidas a través de diferentes canales (**phishing**, smishing y vishing), el fraude con **criptomonedas** o los **ataques a la cadena de suministro** engrosan la lista de recursos delictivos.

"El modelo RaaS para alquilar ransomware como servicio ha ganado popularidad"

> “la IA **ya es un instrumento más para los atacantes**. Estos pueden usarla para desarrollar sus propias herramientas maliciosas y propagarlas”

A esto hay que sumar las amenazas internas, las decisiones de empleados por falta de concienciación sobre ciberseguridad y los incidentes con información privilegiada. Junto a las personas, las máquinas también contribuyen a la diversificación de las amenazas. El alcance de la ciberdelincuencia se amplía por medio de los vectores de ataque que ofrece el internet de las cosas. Los **dispositivos IoT** están presentes en todo el mundo, con más de 13 000 millones de objetos, desde wearables y televisores hasta termostatos, alarma de humo o cámaras de vigilancia. Cualquier fallo de protección en ellos puede poner en peligro toda la red.

Otro avance tecnológico que está siendo aprovechado por los maleantes es la **inteligencia artificial** (IA), cuyo uso se democratiza a través de soluciones como los chatbots, modelos de lenguaje extenso y la IA generativa. Además de facilitar las interacciones con usuarios o la creación de contenido nuevo desde cero, la IA **ya es un instrumento más para los atacantes**. Estos pueden usarla para desarrollar sus propias herramientas maliciosas y propagarlas.

Su alcance incluye las **noticias falsas** para engañar hasta a los internautas más sensatos y que hacen tambalear la confianza democrática. La desinformación tiene potencial para activar la guerra psicológica. Las **botnets** son otro elemento que hay que tener en cuenta en el complejo panorama mundial, ya que la IA permite automatizar sus ataques. Los adversarios de las empresas en el ciberespacio se organizan en **bandas sofisticadas que combinan la intervención humana y la automatización**, con capacidades integradas de aprendizaje automático.

La repercusión de los lances de seguridad se ha ampliado y compromete activos sensibles de los negocios, empezando por aquellos datos que sus clientes han compartido en confianza. La protección y la **gestión de riesgos, con la posibilidad de responder** a los continuos envites de los ciberdelincuentes, debe ser la **prioridad número uno** de las organizaciones, privadas y públicas

Soluciones XDR y EDR para detección y respuesta

"La tecnología XDR tiene una propuesta de detección y respuesta extendidas que plantea una cobertura mayor al reunir varias soluciones de seguridad en una única plataforma"

Que las ciberamenazas son cada vez más refinadas es una realidad y plantean **retos imposibles de resolver para los tradicionales antivirus**. Las compañías no pueden seguir dependiendo de medidas que no han sido pensadas para afrontar la complejidad actual. Tampoco pueden apostarlo todo a la neutralización gestionada por humanos. Para blindar su infraestructura frente a amenazas previamente desconocidas y ciberataques fulgurantes como los del ransomware necesitan nuevas tecnologías que sean capaces de ejecutar la detección y la neutralización en tiempo real.

La tecnología **eXtended Detection and Response (XDR)** llega para dar solución a esta necesidad. Su propuesta de **detección y respuesta extendidas** plantea una cobertura mayor al reunir **varias soluciones de seguridad en una única plataforma**. Con un diseño **multicapa**, apunta a los incidentes que van surgiendo en diferentes frentes como la red, la nube, el correo electrónico o los endpoints, gracias al intercambio de información y el entramado de relaciones que se establecen entre los productos.

Esto le permite plantear un enfoque más preciso, combatiendo la fatiga de las alertas. Su amplia gama de fuentes es una de sus ventajas. XDR cuenta con características lo suficientemente elaboradas como para incrementar el nivel de **contextualización** y anticiparse a consecuencias fatales. Puede cruzar información técnica con contenidos externos y afinar el proceso hasta la **hiperauto-matización**. Descubre, analiza, pone en cuarentena y remedia sin perder un segundo.

Para seguir el ritmo a un entorno en constante evolución, los equipos de seguridad de las empresas precisan de toda la ayuda que puedan recibir. Con soluciones innovadoras y de manejo intuitivo podrán gestionar mejor su tiempo y centrarse en tareas de valor añadido. Lo más recomendable es centralizar la información y configurar una **visión holística** que facilite el análisis y contenga los puntos ciegos.

Una de las bases sobre las que se construyen las herramientas de detección y respuesta es el **EDR**. Esto es, la **detección y respuesta en los terminales** (Endpoint Detection and Response). O, lo que es lo mismo, un agente que recoge y analiza variaciones que pueden terminar en un compromiso a nivel de endpoint y, por tanto, para el resto del sistema de información al que se encuentra conectado. A diferencia de otras alternativas, **no depende en exclusiva de un modelo basado en firmas** para descubrir las amenazas que acechan a los negocios.

El EDR, que hace un uso respetuoso de la IA, parte de **patrones de comportamiento** e identifica anomalías cuando recopila los datos telemétricos y de funcionamiento de los dispositivos y los correlaciona para abordar el problema. Interviene con análisis e investigaciones profundas para llevar a cabo la remediación. Esta protección para endpoints permite compensar las lagunas que están presentes en herramientas de seguridad básicas en un mundo que se ha vuelto complicado.

MTD: La defensa que el móvil necesita

Uno de los terminales más utilizados en la actualidad, también en el ámbito corporativo, es el **smartphone**. El teléfono móvil inteligente sirve para todo. Permite ponerse en contacto por medio de llamadas o mensajería instantánea, enviar emails, unirse a reuniones por vídeo, acceder a documentos compartidos, realizar grabaciones, realizar pagos, autenticarse y un sinfín de tareas más.

Esto significa que **la información que se almacena** y descarga en este tipo de aparato **es sensible**. La lista de contactos es un bien codiciado por los cibercriminales, para expandir sus ataques entre el mayor número de personas posible. Un smartphone puede dar acceso a correos que se han intercambiado con clientes y proveedores, proyectos profesionales que todavía no han salido a la luz y otros activos de la compañía para la que trabaja su propietario. Como contenedores de todos estos datos, los móviles de las empresas deberían estar más protegidos que nunca.

Al igual que ocurre con los ordenadores de sobremesa, **los teléfonos necesitan ser reforzados con soluciones de seguridad**, algo que muchos usuarios olvidan.

Solo así mantendrán alejados a los delincuentes cibernéticos. No importa el sistema operativo que utilicen, existen ejemplares de malware que han sido concebidos para todos los escenarios imaginables y que intentarán con afán encontrar el resquicio por el que colarse. Y habrá aplicaciones que se saltarán los protocolos de las tiendas y engañarán a los usuarios para proceder a su instalación.

La tecnología **MTD** (Mobile Threat Defense o **defensa frente a amenazas móviles**) pone freno al software malintencionado. Examina las apps, incluyendo las aplicaciones del sistema, a medida que estas se instalan y se van actualizando para blindar el parque móvil de las empresas. Esta solución específica para teléfonos contiene los ataque de fuerza bruta, man-in-the-middle y las tentativas de aprovechar vulnerabilidades en la configuración local.

Entre sus capacidades se encuentran las **listas negras**, el análisis de código estático y dinámico, así como la **revisión de los permisos** concedidos al software. También caben posibilidades como el **escaneo en busca de jailbreak**, la detección de procesos de depuración ilegítimos o la emisión de **alertas por la conexión con un dominio malicioso**. Al recibir notificaciones de seguridad en tiempo real, los usuarios pueden optimizar su margen de reacción. En la parte de la remediación entran casos como el aislamiento de DNS objetivos y el borrado si se produce una pérdida o el robo del dispositivo.

Una herramienta de este tipo se antoja vital ahora que más personas alrededor del planeta tienen la opción de realizar su actividad en remoto, en un espacio de trabajo híbrido donde el **teletrabajo** gana presencia. Esto va acompañado de la extensión de las políticas **BYOD** (Bring Your Own Device, en español "trae tu propio dispositivo"), que autoriza el uso de aparatos personales para temas profesionales.

"Al igual que ocurre con los ordenadores de sobremesa, **los teléfonos necesitan ser reforzados con soluciones de seguridad**"

Cómo la inteligencia artificial impulsa la seguridad

"Las herramientas de seguridad que recurren a la IA entienden mejor las prácticas de los ciberdelincuentes"

Un ciberataque puede ocurrir en cualquier momento y completar su cometido en cuestión de minutos, por lo que es importante tener la facultad de intervenir al instante. Incorporar como defensa una solución hiperautomatizada que, sin presencia humana de por medio, se oponga a los ataques en tiempo real es la opción ideal para las empresas. **Proactividad y reactividad destacan como cualidades cruciales** y se consiguen por medio de la automatización.

Las amenazas cambian sin cesar para romper las barreras de protección que hay instaladas. **La ciberseguridad es una cuestión dinámica**. Antes las organizaciones combatían malware que había sido desarrollado por personas y contra el que soluciones basadas en firmas y con carácter preventivo eran suficientes. En estos momentos, los ataques son más avanzados, dirigidos y pueden hacer un uso perverso de la inteligencia artificial. Más que nunca, hace falta optimizar la protección y desprenderse de análisis manuales lentos.

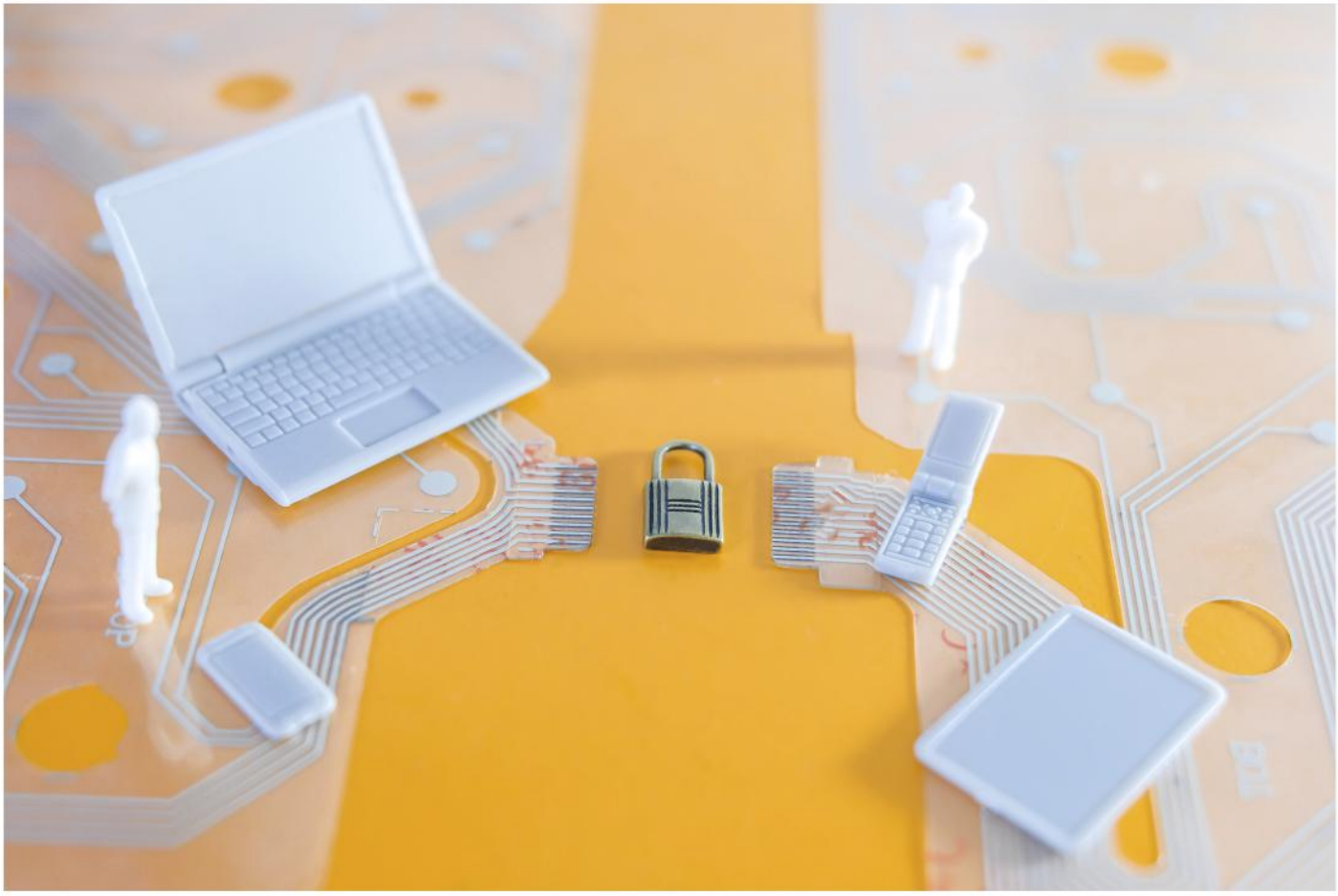
Una solución que monitorice todo el entramado corporativo, incluyendo los terminales móviles de los empleados, con el apoyo de robots de software, detectará anomalías con solvencia, podrá calificarlas y les pondrá fin en el momento preciso. Aquí entra en juego la inteligencia artificial en su faceta más positiva. **La IA aporta velocidad de acción** en el ámbito de la ciberseguridad.

Toma la decisión de bloquear amenazas potenciales antes de que sea tarde y repercuta en las finanzas y la reputación de la compañía. Un ataque exitoso suele derivar en problemas legales y la pérdida de clientes.

Esta tecnología conlleva ventajas como la inmediatez. Gracias a las aportaciones del aprendizaje automático y el aprendizaje profundo, existe una forma eficaz y veloz de responder a la rapidez con la que están evolucionando las ciberamenazas. Las herramientas de seguridad que recurren a la IA entienden mejor las prácticas de los ciberdelincuentes y detectan **aspectos sutiles de las amenazas que resultan invisibles a simple vista.**

Las empresas pueden, y deben, combatir con las mismas armas que los agentes malignos tienen a su alcance. La IA se nutre con volúmenes ingentes de datos para orientar sus acciones, y lo hace a un ritmo frenético que las personas que forman parte de los equipos de protección no podrían seguir por su cuenta, ni siquiera uniendo esfuerzos. También aprende y mejora con la experiencia, por lo que su espacio de mejora en el enfrentamiento con los criminales es constante. No se queda desfasada. Es una tecnología que se enfrenta a amenazas desconocidas, anticipa riesgos y sortea hipotéticos escenarios de derrota.

La diversidad de dispositivos, sistemas y entornos en estos momentos reclama una solución con interconexión y que evolucione conforme lo va haciendo el estado de las ciberamenazas. La idoneidad de la IA es compartida por todos los sectores y compañías, empezando por las de dimensiones reducidas y terminando por la industria, donde detener la producción para parchear es imposible.



Más visibilidad, más protección

Bancos, firmas de seguros, entidades educativas, el segmento energético, los centros de atención médica... desde el primer sector al último corren peligro de caer en las redes de los hackers. Eludir la protección de una organización y tomar el control de sus equipos, sobre todo si los **datos** que recopila son especialmente valiosos y se pueden comercializar o emplear para sucesivas embestidas, será la misión de terceros con intenciones espurias. Hay ataques que apuntan directamente a infraestructuras básicas, como las redes eléctricas, o a sistemas de domótica.

Para impedir un desastre digital, lo aconsejable es potenciar la visibilidad y promover el modo de remediación, no solo de detección. Esto se consigue mediante la integración en una única plataforma de herramientas de seguridad enfocadas a diferentes áreas de actuación. Y, en mayor medida, con **una consola unificada que aglutine y relacione entre sí cada módulo** para ofrecer a los responsables de seguridad **una visualización de 360 grados**.

Una de las peores cosas que puede suceder en la lucha cibernética es actuar a ciegas o con un fragmento aislado de información, porque el análisis pecará de inexactitud y conducirá a error. Los módulos de una solución XDR consisten en sensores inteligentes que están integrados en los activos digitales y que trabajan con los datos en un único sitio para proporcionar a los expertos una visión **holística** de la situación con la que trazar una composición de lugar.

Las herramientas EDR y MTD forman parte de este conjunto de adelantos técnicos para asegurar teléfonos, tabletas, ordenadores y servidores. Con **NTA** se supervisan los flujos de tráfico de red. Una solución **SIEM** para la gestión de información ayuda a guardar todos los registros de eventos relacionados con el entorno del cliente. Y un módulo de respuesta engañosa delatará a los atacantes.

Todas estas piezas se comunican entre sí con la fórmula de **SOAR** (orquestación, automatización y respuesta de seguridad) y entregan a los analistas la información que necesitan para realizar su trabajo con propiedad. Con la implementación de la tecnología, los profesionales de la ciberseguridad elevan el ratio de éxito a su alcance. Pueden preparar a sus empresas para el combate y plantear acciones de mitigación cuando sea preciso. El sistema se alimentará a sí mismo y mejorará a partir de sus propios descubrimientos.

Prever acontecimientos a través de un sistema automatizado que funciona de manera incansable y en todo lugar confiere a las organizaciones un recurso poderoso en tiempos de guerra cibernética. Ante las limitaciones de las soluciones heredadas, la saturación de los empleados y una falta de talento que merma a las empresas, los nuevos desarrollos refuerzan la protección. Esto es fruto de una **innovación constante**.

> "lo aconsejable es potenciar la visibilidad y promover el modo de remediación, no solo de detección"

TEHTRIS tiene la respuesta

"La **hiperauto-matización** acelera los procesos y evita que las compañías tengan que depender de decisiones incompletas"

El grado de innovación que se ha alcanzado en el área de la inteligencia artificial permite fortalecer la ciberseguridad. La plataforma **TEHTRIS XDR** cumple con los requisitos de las empresas actuales de visibilidad, instantaneidad, simplicidad y protección eficaz a través de su propuesta de **neutralización automática de ciberataques en tiempo real y sin intervención humana.** Esta plataforma de detección y respuesta extendidas capacita a los equipos de TI de organizaciones de todos los tamaños y sectores para afrontar lo inesperado.

TEHTRIS está preparada para los retos del presente y también del futuro. **Compuesta por diferentes módulos de seguridad, incluyendo EDR, MTD, SIEM, NTA, DR (Honeypots) o DNS Firewall**, su solución va sumando capacidades nuevas con frecuencia. Todos estos componentes **están interco-nectados y son controlados por el motor de inteligencia artificial CYBERIA**, que simplifica la búsqueda de puntos débiles en grandes infraestructuras distribuidas al reconocer comportamientos anómalos. El **SOAR integrado** permite establecer interacciones entre sensores inteligentes y bloquear las amenazas.

La **hiperautomatización** es uno de sus grandes pilares, ya que acelera los procesos y evita que las compañías tengan que depender de decisiones incompletas, que no han examinado los datos en profundidad o con una base poco sólida.

Esto, a su vez, reduce los falsos positivos que entorpecen las tareas de protección. La infraestructura está vigilada en todo momento y los ataques de los ciberdelincuentes se abordan con premura.

Esta plataforma TEHTRIS XDR dispone de tecnología para la gestión de filtros y capacidades de coedición, de modo que los analistas pueden colaborar y ahorrar tiempo durante las investigaciones y la respuesta a incidentes. En la práctica, **los expertos que sufren una sobrecarga de funciones se libran de las tareas más repetitivas** y tienen la oportunidad de centrarse en sus prioridades de seguridad.

A esto contribuye la monitorización 24/7 y una **consola unificada** que TEHTRIS ha diseñado tanto para gestionar sus herramientas como la integración con terceros, con un listado de más de 400 referencias. Ofrece interoperabilidad de forma nativa con diferentes productos del mercado. La plataforma TEHTRIS XDR también es compatible con múltiples sistemas operativos, aplicaciones y bases de datos. El resultado es una **seguridad 360**.

TEHTRIS trabaja con los logs, los hashes de los dispositivos y las variaciones de comportamiento. Para garantizar la protección de los entornos empresariales y del sector público **no necesita acceder a los ficheros de sus clientes**. Entrega a los especialistas

“TEHTRIS responde en tiempo real. Orquesta herramientas dentro de una única plataforma para obtener una visión global de los sistemas”

en protección cibernética un enfoque holístico de la situación que ayuda a mantener el control, al mismo tiempo que se encarga de preservar la confidencialidad de la información. Esto es así porque el software sigue unas pautas de seguridad y ética por diseño.

Además, la plataforma TEHTRIS XDR es una **solución 100 % europea**, que ha sido desarrollada y se encuentra alojada en Europa, lo que significa que cumple las leyes comunitarias de privacidad de datos y respeta la inviolabilidad del contenido de los archivos que se compromete a proteger. Destaca por el **cumplimiento normativo**, la soberanía y una misión de **transparencia** con las organizaciones privadas y públicas a las que protege. Cuenta con la **certificación ISO 27001** de confidencialidad, integridad y disponibilidad respecto a la gestión de seguridad de la información.

La solución está **alojada en la nube** y también está disponible on-premise. Ha sido diseñada sin capas de software preexistentes en su objetivo de luchar contra el ciberespionaje, el cibersabotaje y el crítico panorama de amenazas mundial. El crecimiento incesante de la ciberdelincuencia alrededor del planeta es un reto decisivo. TEHTRIS tiene la respuesta. Sabe cómo hacerle frente supervisando, detectando, analizando y bloqueando tentativas de ataque y fallos de seguridad en todas las industria. Esto es, desde la banca o el retail a salud, educación y Administración pública.

Desde el cloud hasta los terminales, la tecnología de TEHTRIS responde en tiempo real a problemas como el ransomware o los ataques de Día Cero para que sus efectos no vayan a más. Orquesta herramientas dentro de una única plataforma para obtener una visión global de los sistemas corporativos, una colaboración optimizada entre equipos de profesionales y una reactividad total. Es respetuosa con los datos. Y, sobre todo, pone la **inteligencia artificial** a trabajar **en favor de la ciberseguridad**.

FACE THE UNPREDICTABLE

CONTACTA CON NOSOTROS

spain@tehtris.eu

www.tehtris.com

MADE IN EUROPE