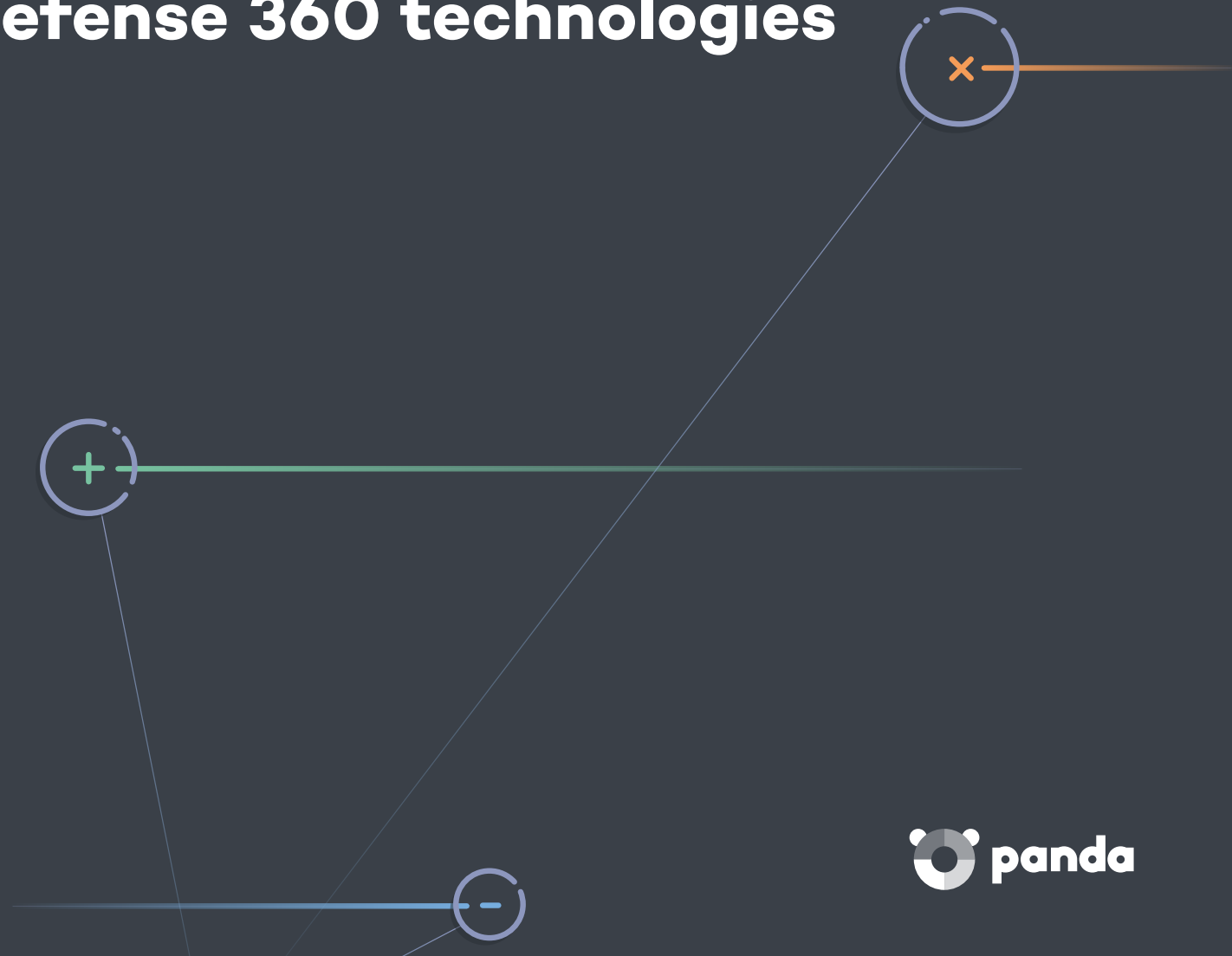
Panda Adaptive Defense 360 technologies

Managed Detection,

Managed Mitigation



pandasecurity.com

panda

Adaptive Defense 360

Índice

1. Tecnologías y servicios de Panda Adaptive Defense 360.

Introducción

En este documento se explica la cooperación de las **tecnologías y servicios gestionados integrados en Panda Adaptive Defense 360**, en las que las capacidades de Endpoint Detection and response (EDR) y la aplicación de tecnologías de Inteligencia Artificial a la seguridad, son factores diferenciadores.

El siguiente diagrama muestra dónde se aplica cada tecnología y qué tipo de técnicas funcionan con el fin de bloquear a los adversarios lo antes posible, evitando que los endpoints se vean comprometidos, detectando, conteniendo y respondiendo a los atacantes antes de que se produzca el daño.

Panda Adaptive Defense 360

Unattended & Managed services	PREVENT	DETECT	HUNT	INVESTIGATE/ FORENSIC	CONTAIN/ REMEDIATE	ANTICIPATE Avoid Future Attacks
KNOWN & UNKNOWN MALWARE	Traditional EPP technologies [1] 100% Attestation Services [2] Risk-based Application Control: Lock/Hardening mode			Incident Analysis, Event timeline	Execution denied, Managed disinfection	Incident analysis insights Panda Patch Management Advanced Reporting tool Panda Data Control
EXPLOITS Metaexploits, Exploits kits, Exploits in the wild	Pre-execution IoAs of exploits in the wild[3]	Behavioral IoAs in memory[4]	Threat Hunting & Investigation Service (THIS)[7] Feeds new IoAs to the endpoint agents		Compromised process killed, Isolate endpoints	
LIVIN-OFF-THE-LAND High confidence malicious activity	Context based pre-execution IoAs (Interpreters, scripts, macros)[5]	Behavioral IoAs with admin tools, scripts, shellcode injections[6]			Execution denied or blocked	

A continuación, se detallan estas tecnologías y servicios de prevención, detección y respuesta:

1. **Tecnologías preventivas** de Protección Endpoint (1).
2. **Servicio gestionado, 100% Attestation Service** (2), que clasifica todas las aplicaciones y binarios antes y durante su ejecución, para asegurar que solo aquellos confiables puedan ejecutarse.
3. **Tecnologías de detección de explotaciones de aplicaciones y técnicas living-off-the-land** (3, 4, 5, 6). Las técnicas de ataque LotL permiten al atacante aprovechar las aplicaciones administrativas preexistentes en los dispositivos y servidores y hacer un uso indebido de ellas, pasando inadvertidos.
4. **Servicio gestionado de Threat Hunting** (7), incluido en la solución, donde expertos en seguridad descubren nuevas técnicas lotL e incorporan su detección en el endpoint.

2. Stack de Tecnologías EPP

EPP Proactive Technologies Stack	Panda Adaptive Defense 360
Generalist signatures and Heuristics	✓
Cloud Based Lookup to the Collective Intelligence (Threat Intel)	✓
Behavioral analysis & IoAs detection	✓
Firewall, IDS/IPS, Networks packet inspection	✓
Anti-tampering	✓
Device Control	✓
URL Classification & Reputation	✓
Application Control	✓
Antispam, Antiphishing, content filtering for MS Exchange Servers	✓
Mailbox protection & Intelligence Scan for MS Exchange Servers	✓
Vulnerability Assessment & Patching*	✓

*Panda Patch Management

Existe en el mercado la creencia incorrecta de que las tecnologías EPP (Endpoint Protection Platform) son básicamente un análisis basado en firmas y que no son necesarias cuando se protegen los endpoint con soluciones EDR.

Estás tecnologías combinan además de las firmas diferentes técnicas de detección como firmas genéricas, heurísticas, firewall, reputación de URLs, análisis de comportamiento e Indicadores de Ataque (IoAs), gestión de vulnerabilidades, control de aplicaciones y otras capacidades que reducen la exposición al riesgo.

Estas tecnologías preventivas cooperan con las soluciones EDR, aportando:

- **Reducción significativa el riesgo**. No necesitan ejecutar un fichero para detectar, en ejecución, que es malicioso y no necesitan conectividad, salvo para consultar a la nube.

- **Bajos niveles de falsos positivos.** Las tecnologías EPP, de las que se espera que protejan de forma autónoma y distribuidas en gran volumen de endpoints, no admiten falsos positivos.

- **Optimización en el endpoint.** Estas tecnologías cooperan entre sí, para evitar redundancias y penalizar lo menos el rendimiento de los endpoints que protegen.

3. El servicio 100% Attestation.
La Inteligencia Artificial: innovación disruptiva en la seguridad

Como parte de la licencia de Panda **Adaptive Defense y Adaptive Defense 360**, se incluye un servicio gestionado que clasifica en malware o confiable todos los procesos que se ejecutan en cada endpoint, su gran ventaja es que asegura que solo los que son confiables se ejecuten. Siendo un servicio totalmente automatizado, no requiere de la intervención o decisión por parte del usuario final, el equipo de seguridad o de IT.

El servicio 100% Attestation service está compuesto por tres componentes clave:

1. **Monitorización continua en endpoint desde la plataforma nativa en la nube.**

   La actividad de cualquier aplicación en los endpoints, independientemente de su naturaleza, es monitorizado y enviado a la nube para su clasificación continua. Gracias a ello se previene la ejecución de malware, incluso los ataques más sofisticados como los "Supply chain Attacks"[1].

   La telemetría recogida esta optimizada, normalizada y filtrada para reducir el impacto en el cliente, siendo enriquecida en la plataforma en la nube para múltiples propósitos, incluida la clasificación, la detección de comportamientos sospechosos y el uso de técnicas maliciosas conocidas y desconocidas.

2. **Clasificación automatizada con IA.**

   La clasificación automatizada está gobernada por un sistema en la nube de Inteligencia Artificial, donde se ejecutan en continuación un array de múltiples de algoritmos de Machine Learning donde se procesan cientos de atributos estáticos, de comportamiento y de contexto de ejecución, en tiempo real. Los atributos se extraen de la telemetría del entorno protegido y de los obtenidos utilizando **Sandboxes físicos.**

   A día de hoy, la tasa de clasificación automatizada es del 99,98%, lo que significa que solo el 0,02% de los procesos necesita la intervención de nuestros expertos, el sistema de Inteligencia Artificial es autosuficiente en su procesamientos en escala en tiempo real, sin falsos positivos y sin requerir de la intervención del usuario final.

¿Qué es un sandboxing físico?

Un array de máquinas físicas configuradas en la nube específicamente para detonar los ficheros y extraer observables en tiempo real de comportamiento y de contexto. Utilizamos Sandboxing físico en lugar de Virtual Machine Sandboxing, porque existen numerosas aplicaciones maliciosas que pueden detectar cuándo se están ejecutando en una VM y no mostrar su comportamiento malicioso.

3. **Control de aplicación basado en el riesgo.**

Se refiere a los modos en que opera el agente de protección en el endpoint, existiendo dos niveles de protección:

- **Modo hardening:** denegación predeterminada de todas las aplicaciones y binarios desconocidos provenientes del exterior (descargas web, correo electrónico, USB, ubicaciones remotas, etc.).

- **Modo bloqueo:** denegación predeterminada de todas las aplicaciones desconocidas, independientemente del origen (de la red, en la máquina y fuera de ellas). Asegura que todos los procesos en ejecución son confiables.

La Inteligencia Colectiva de Panda,

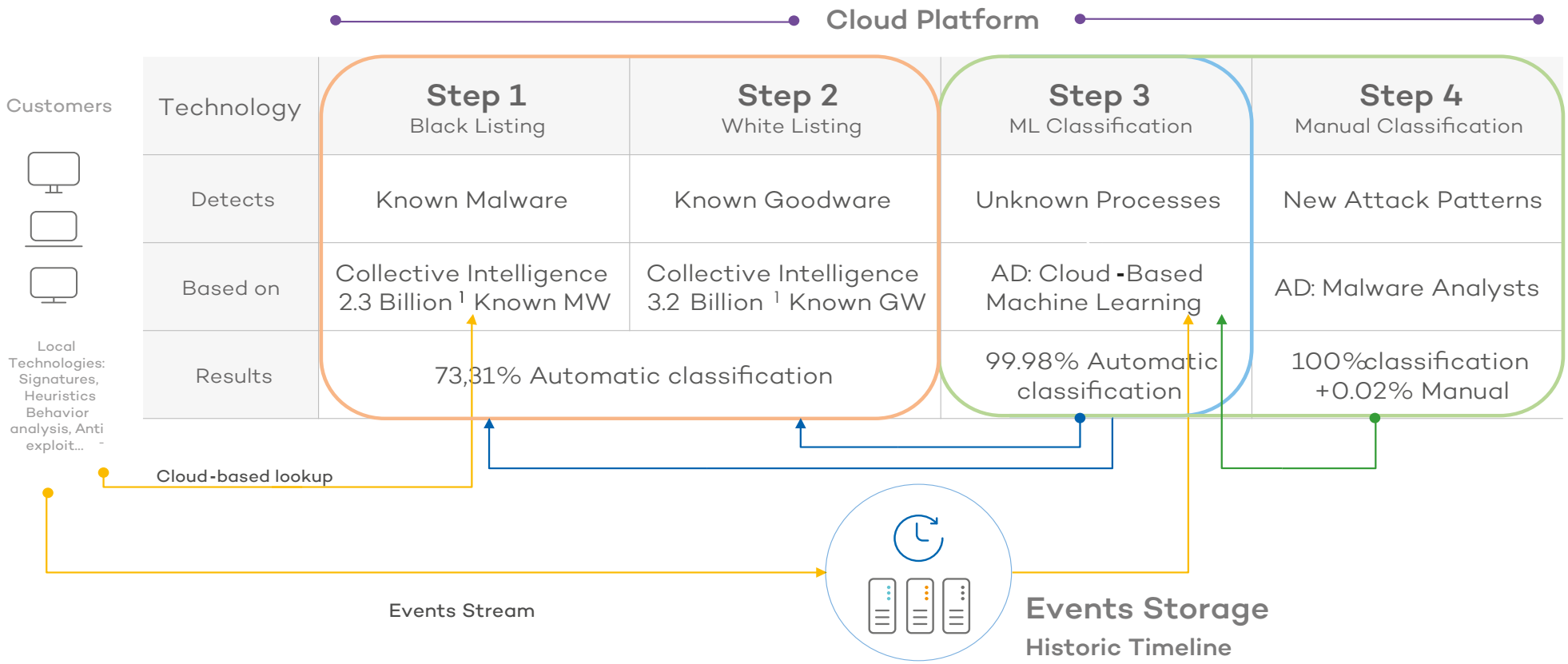
Alojado en la plataforma nube de Panda Security, es otro de los componentes fundamentales que habilita la operativa de este nuevo modelo de protección e incrementa la eficiencia del servicio 100% Attestation.

La Inteligencia Colectiva es el almacenamiento consolidado e incremental del conocimiento de Panda Security, tanto de aplicaciones, binarios y otros ficheros que pueden contener código interpretado confiables como maliciosos.

Este repositorio a escala en la nube es continuamente alimentado por el sistema de Inteligencia Artificial y los analistas expertos y es a la vez consultada por el ecosistema de soluciones y servicios de Panda Security, antes de cualquier ejecución.

El siguiente gráfico muestra la colaboración de stack de tecnologías que gobiernan el buen funcionamiento del servicio de clasificación de todas las aplicaciones, binarios y ficheros interpretados, en tiempo real.

Cómo funciona el servicio de 100% Attestation



4. Protección de explotación de aplicaciones y ataques Living-off-the-land (LotL)

La monitorización continua de la actividad en los endpoints permite al agente en los endpoints actuar como sensor e informar a la plataforma nube de Panda Security no solo de lo que ejecuta, sino también de su contexto de ejecución (que sucedió justo antes, que usuarios están intentando ejecutar cada comando o aplicación, que tráfico de red se está generando, que ficheros de datos están siendo accedidos, parámetros, etc).

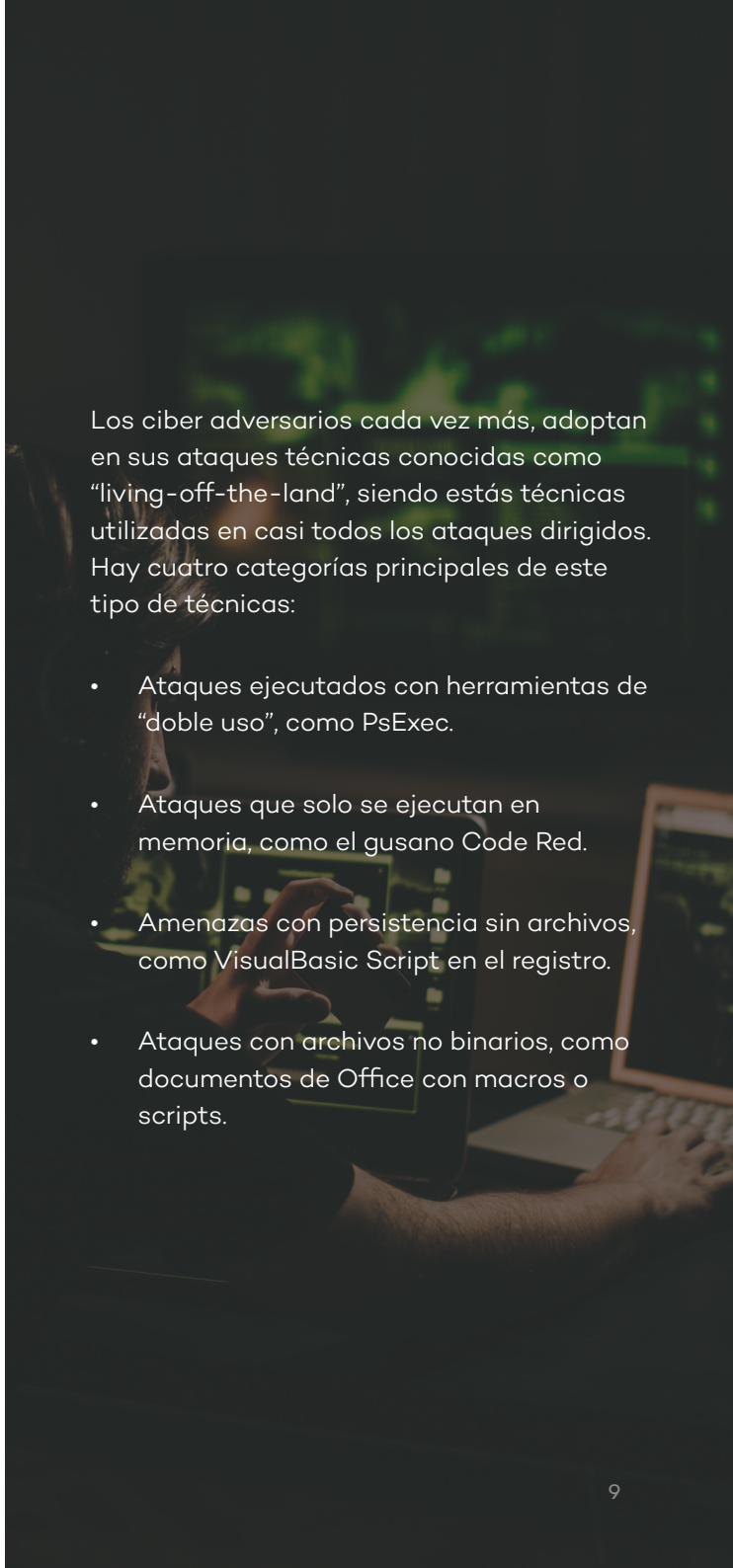
Todo ello permite la identificación, en primera instancia en el endpoint, de comportamientos anormales o sospechosos y categorizarlos como Indicadores de Ataque (IoAs) con una alta confianza y sin falsos positivos.

En muchas ocasiones, los IoAs están asociados a fases concretas de la **Cyber Kill Chain** o tácticas en el framework **ATT&CK de MITRE**[2]:

- Acceso Inicial.
- Ejecución.
- Persistencia.
- Escalado de privilegios.
- Evasión de los controles de defensa.
- Acceso a credenciales.
- Descubrimiento.
- Movimiento lateral.
- Recolección.
- Command and Control (CC).
- Exfiltración.
- Impacto.

La detección de IoAs, en fases previas a la exfiltración de datos o cifrado, en el caso de ransomware, aun existiendo un compromiso de los endpoints, es un mecanismo de defensa muy eficaz, en especial contra los ataques de tipo "living-Off-the-land" (LotL).

Nuestras soluciones Panda Adaptive Defense y Panda Adaptive Defense 360 incorporan en el agente de protección un stack completo de tecnologías para la detección de IoAs en diferentes fases del ataque. Lejos de ser tecnologías estáticas, estas se actualizan en continuación con nuevos patrones de técnicas de ataque que el servicio de Panda Security, THIS, detecta.



Los ciber adversarios cada vez más, adoptan en sus ataques técnicas conocidas como "living-off-the-land", siendo estás técnicas utilizadas en casi todos los ataques dirigidos. Hay cuatro categorías principales de este tipo de técnicas:

- Ataques ejecutados con herramientas de "doble uso", como PsExec.
- Ataques que solo se ejecutan en memoria, como el gusano Code Red.
- Amenazas con persistencia sin archivos, como VisualBasic Script en el registro.
- Ataques con archivos no binarios, como documentos de Office con macros o scripts.

Entre los numerosos Indicadores de Ataque que el agente detecta, encontramos las siguientes categorías:

1. IoAs de exploits in the wild

Mediante esta tecnología se detectan y bloquean, en pre-ejecución, IoAs de comportamiento y contexto tanto de antiexploits en the wild como exploits kits, cerrando con ello, unos de los vectores principales de riesgo de entrada en las máquinas.

A esto se añaden tecnologías propietarias de firewall para implementar la capacidad de **Virtual Patching** en el endpoint, detectando y bloqueando con este mecanismos, intentos de explotación de vulnerabilidades observando el tráfico de entrada.

Un ejemplo de reglas de firewall puede ser las que identifican y bloquean explotaciones EthernalBlue, donde en un ataque BlueKeep se establecen comunicaciones específica dentro de una sesión RDP. Estas conexiones hacen que el controlador del sistema operativo se bloquee permitiendo una ejecución remota de código (RCE).

La tecnología Firewall, detecta esta comunicación RDP específica y la rechazando automáticamente. La detección se registra en la nube es presentada en la consola web en Panda Adaptive Defense 360, una nueva detección que obliga a la toma de acción urgente por los administradores.

Estos deben, como medida de contención, aplicar los cambios necesarios en la configuración para contener el ataque, activando la autenticación de nivel de red (NLA) y deshabilitando el servicio de escritorio remoto en aquellos endpoints donde su uso no sea esencial, y en paralelo reducir la superficie de ataque actualizando lo antes posibles los sistemas (si esto es posible).

2. IoAs en la memoria: tecnología antiexploits dinámica

Panda Adaptive Defense 360 incorpora una tecnología antiexploits dinámica.

Esta tecnología, totalmente independiente a las técnicas implementadas en Microsoft EMET, no pivota alrededor de un análisis morfológico de los archivos, o la implementación capas de protección añadidas a las ausentes en Windows (técnicas ASR, DEP, EAF, etc.) o detecciones específicas de vulnerabilidades conocidas. Estas estas técnicas no son suficientes para detener ciberataques diseñados para aprovechar los vectores de entrada creados con vulnerabilidades de día cero.

La tecnología antiexploits dinámica monitoriza el comportamiento interno de los procesos comprometidos, buscando anomalías de su comportamiento convirtiéndose en indicios de compromiso. Este modelo es altamente eficiente en la detección de amenazas independientemente del exploit utilizado en el ataque.

Esta se complementa con una tecnología propietarios de **análisis del framework de memoria**, que inspecciona parte de la memoria en determinados momentos tras un trigger determinado como un evento o un comportamiento sospechoso en busca de Indicadores de compromiso y patrones de ataques de diferente naturaleza en memoria.

Estas tecnologías protegen eficazmente contra **todos tipo de exploits,** especialmente los exploits de **día cero** que se aprovechan de:

- **Vulnerabilidades de navegadores web** en Internet Explorer, Firefox, Chrome, Opera y otros.
- **Familias de aplicaciones objeto de ataques dirigidos:** entre otros muchos Java, Adobe Reader, Adobe Flash, Microsoft Office, reproductores multimedia, etc.
- **Vulnerabilidades en sistemas operativos** no soportados, como Microsoft XP y otros.

3. IoAs en base al contexto en técnicas Living-off-the-land y herramientas administrativas.

Para la detección de este tipo de indicadores, se correlacionan por ejemplos los eventos de cualquier script ejecutado a su vez por un intérprete de scripts de forma que se detecten así ataques con scripting e intérpretes (Powershell, Visual Basic, JavaScripts, etc), toda la suite de MS office (macros/scripts), toda la actividad asociada a WMI, etc.

Otra de las técnica aplicadas, entre otras, deniega la ejecución de procesos por otros según su contexto de ejecución, bloquean así, intentos de ataques sin malware mediante el uso de algunas herramientas administrativas y secuencias de comandos. También permiten detectar ciertos ataques en memoria, por ejemplo, detecciones de inyección de código en la memoria sin archivo presente en el disco.

5. El Servicio Threat Hunting:
Revelando lo indetectable

El servicio de Threat Hunting & Investigation (THIS), Incluido en Panda Adaptive Defense y Panda Adaptive Defense 360, es operado y administrado enteramente por los analistas expertos de Panda Security.

Estos operan una plataforma nativa nube y propietaria de Threat Hunting, investigación y respuesta como el marco para coordinar las tareas de expertos en seguridad de Nivel 1, Nivel 2 y 3, Hunter e Incident Responders que minimizan el MTTD y MTTR (Mean Time to Detect y el Mean Time to Respond) en nuestros clientes.

Los analistas generan nuevas reglas y correlaciones que representan indicios de comportamientos anómalos (IoAs). Estos IoAs, de alta confiabilidad, son entregados inmediatamente en los endpoints protegidos, deteniendo así, lo antes posible, a los adversarios, que pasan inadvertidos a otros controles, con técnicas fileless, LotL, entre otras.

Estos nuevos indicadores de ataque son el resultado del proceso continuo de búsqueda de threat actors existentes en la red de nuestros clientes con técnicas avanzadas a escala de tecnologías de analítica de datos, Threat Intelligence propietaria y la experiencia de nuestros analistas.

Este servicio hereda toda la ciber inteligencia que hemos perfeccionado gracias a nuestros años de experiencia en la investigación de amenazas, la visibilidad histórica que ofrece el registro del comportamiento de aplicaciones, usuarios y máquinas en más de 30 años y nuestras alianzas con organizaciones internacionales como por ejemplo la Cyber Threat Alliance, donde intercambiamos Indicadores de Amenazas (IoAs e IoC) y sus respuestas correspondientes.

6. Certificados, reconocimientos y contribuciones

Panda Security participa regularmente y obtiene premios en protección y rendimiento de Virus Bulletin, AV-Comparatives, AV-Test, NSSLabs. Panda Adaptive Defense logró la certificación EAL2 + en su evaluación para el estándar Common Criteria.

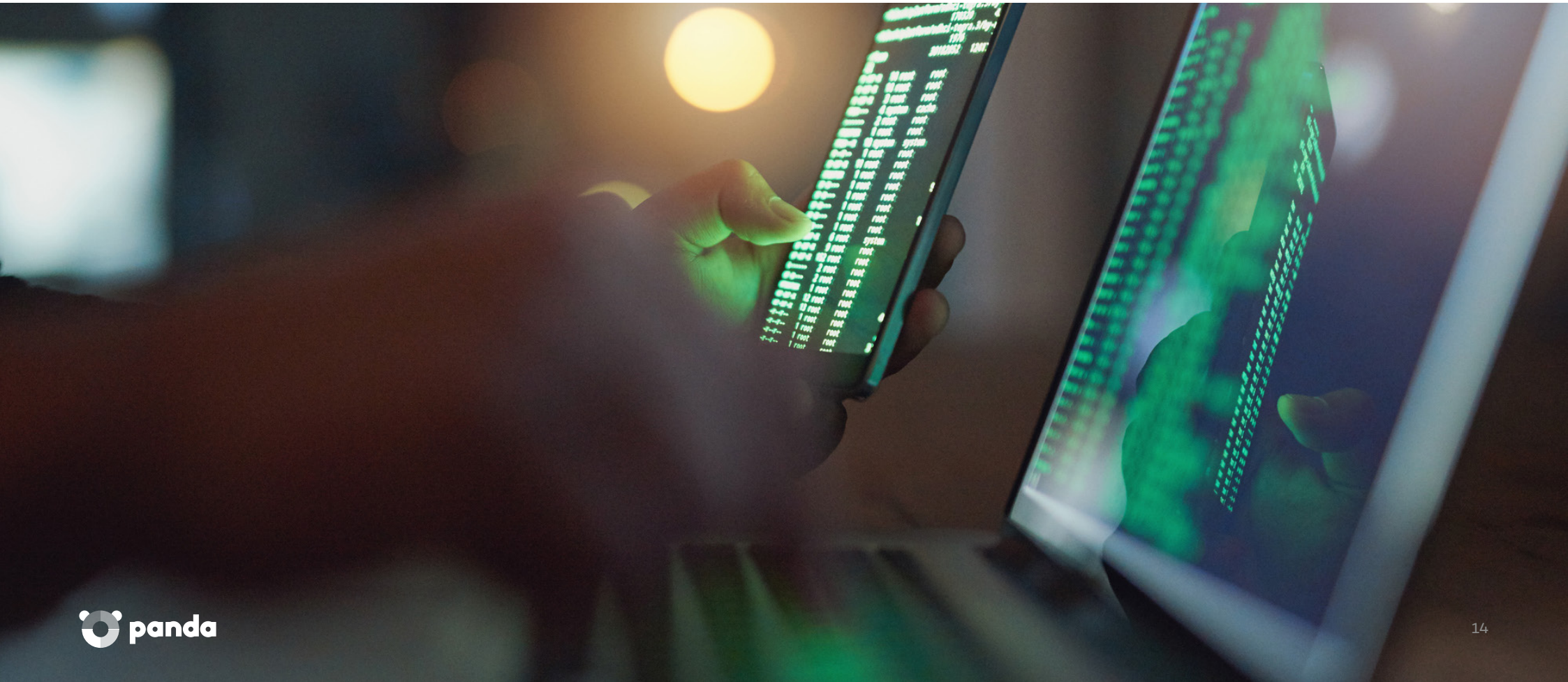
Panda Security reconocido como visionario en el Cuadrante Mágico de Gartner de Endpoint Protection Platforms (EPP) 2018.

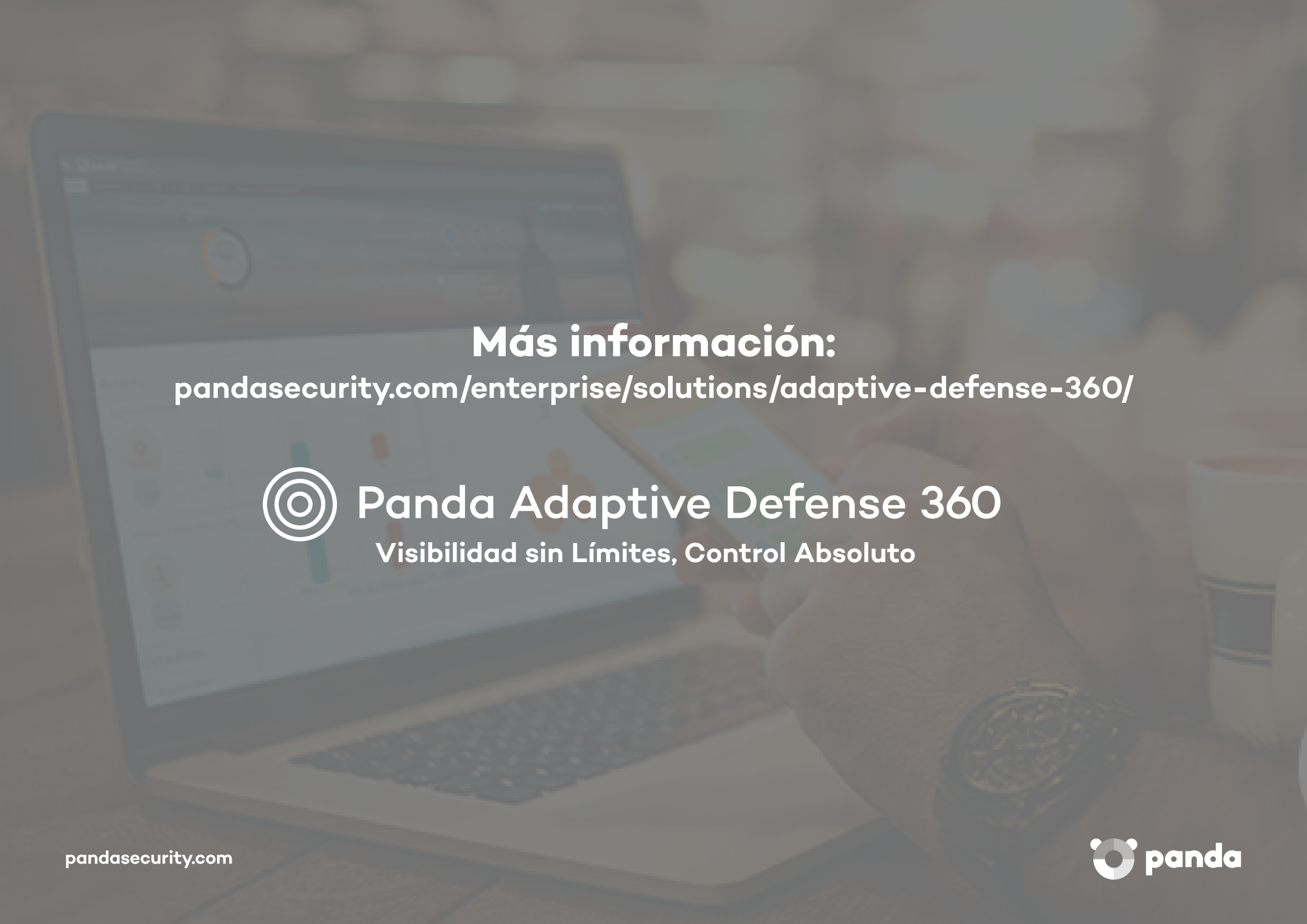
CONTRIBUTING MEMBER

Notas:

1. Los ataques a la cadena de suministro son una amenaza emergente que se dirige a los desarrolladores y proveedores de software. El objetivo es acceder a los códigos fuente, crear procesos o actualizar mecanismos infectando aplicaciones legítimas para distribuir malware

2. Framework de MITRE ATT&CK: **https://attack.mitre.org/**





Más información:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Panda Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

panda