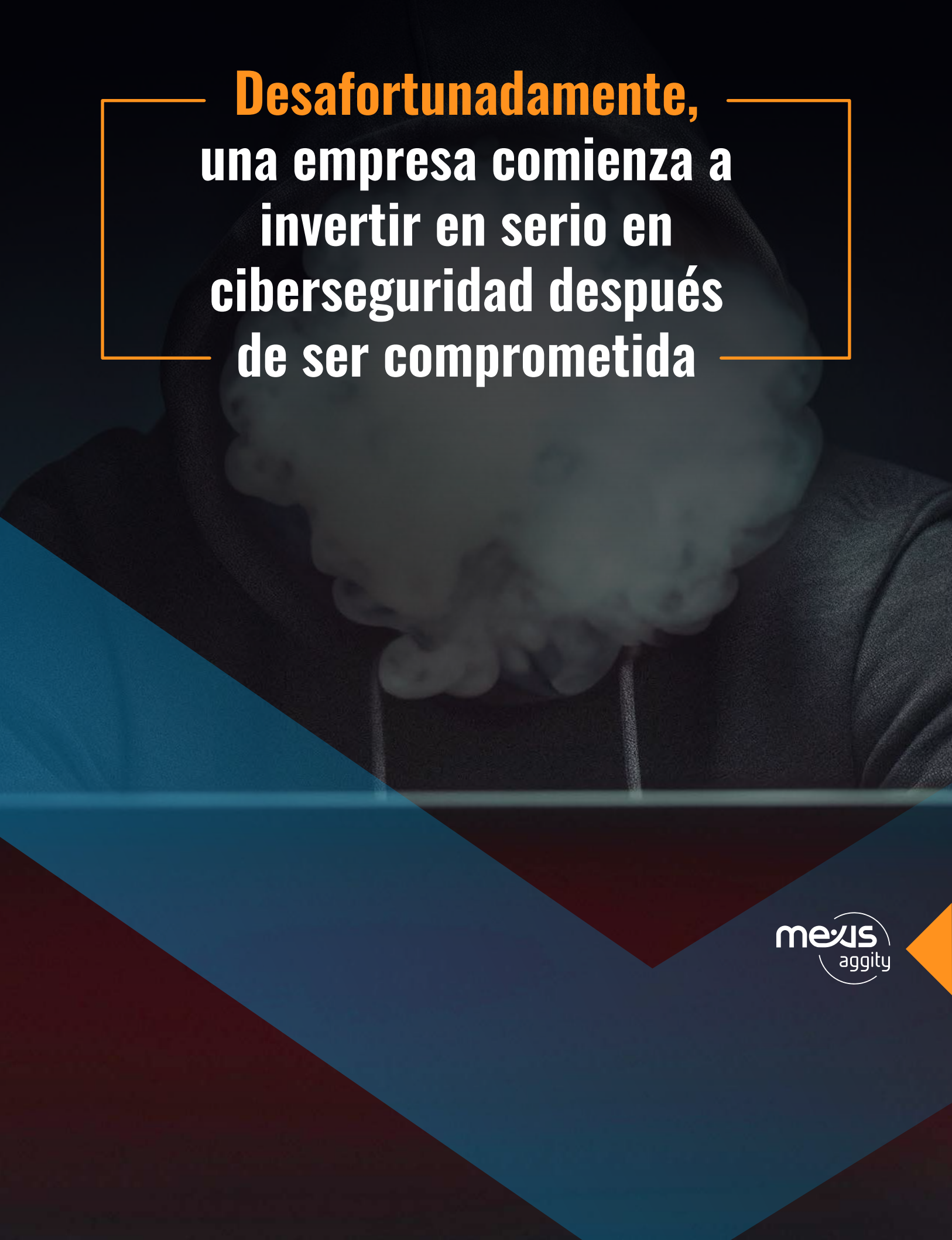


Desafortunadamente,
una empresa comienza a invertir en serio en ciberseguridad después de ser comprometida

mexus aggity

Threat Hunting es la actividad orientada a la búsqueda proactiva de amenazas en el entorno IT de las organizaciones, allí donde no han llegado nuestras herramientas de detección (esto es, donde no se ha producido una alerta).

Se apoya en soluciones de Ciberseguridad de recolección de eventos (event logs de los endpoints, SIEM o tecnología E/XDR) para localizar trazas de actividad sospechosa en el entorno. **Los Threat Hunters son expertos en las técnicas, tácticas y procedimientos de los ciberatacantes.** Aprenden cómo actúan para aplicar este conocimiento en los controles de seguridad y facilitar más su detección, contribuyendo notablemente a la prevención de incidentes. En MuySeguridad hemos entrevistado a Jose Miguel Gómez-Casero Marichal, Threadhunter en SIX/BME.

¿Cuál es el papel del Threat Hunting en la estrategia de ciberseguridad de una compañía? ¿Y cómo ha evolucionado la adopción de estos perfiles en los últimos años?

(Jose Miguel Gómez-Casero Marichal)
El Threat Hunting ayuda a cubrir el espacio existente entre las capacidades de la tecnología de detección de amenazas y los adversarios, haciendo posible la detección y prevención de incidentes para aquellas amenazas donde la tecnología podría no llegar.

También ayuda a comprender con mayor detalle qué ocurre en tu entorno corporativo a nivel de red y endpoints, y entender desde un enfoque ofensivo, cómo pueden comprometer tu organización.

¿Qué papel está jugando ahora mismo la ciberseguridad en los procesos de digitalización de las empresas? ¿Dirías que a partir de la pandemia se ha convertido en la principal prioridad?

(Jose Miguel Gómez-Casero Marichal) Con la consolidación de los modelos de teletrabajo tanto híbridos como completos, la ciberseguridad ha adquirido mayor relevancia, al tener que dar protección no solo en la infraestructura de las oficinas de la empresa, sino en las conexiones que hagan los empleados de sus hogares.

Desafortunadamente, desde mi punto de vista todo ha sido un “boom” tras la pandemia, y en cierto modo hemos vuelto a la misma metodología que antes de la crisis del COVID-19: **una empresa empieza a invertir en serio en ciberseguridad después de ser comprometida.**

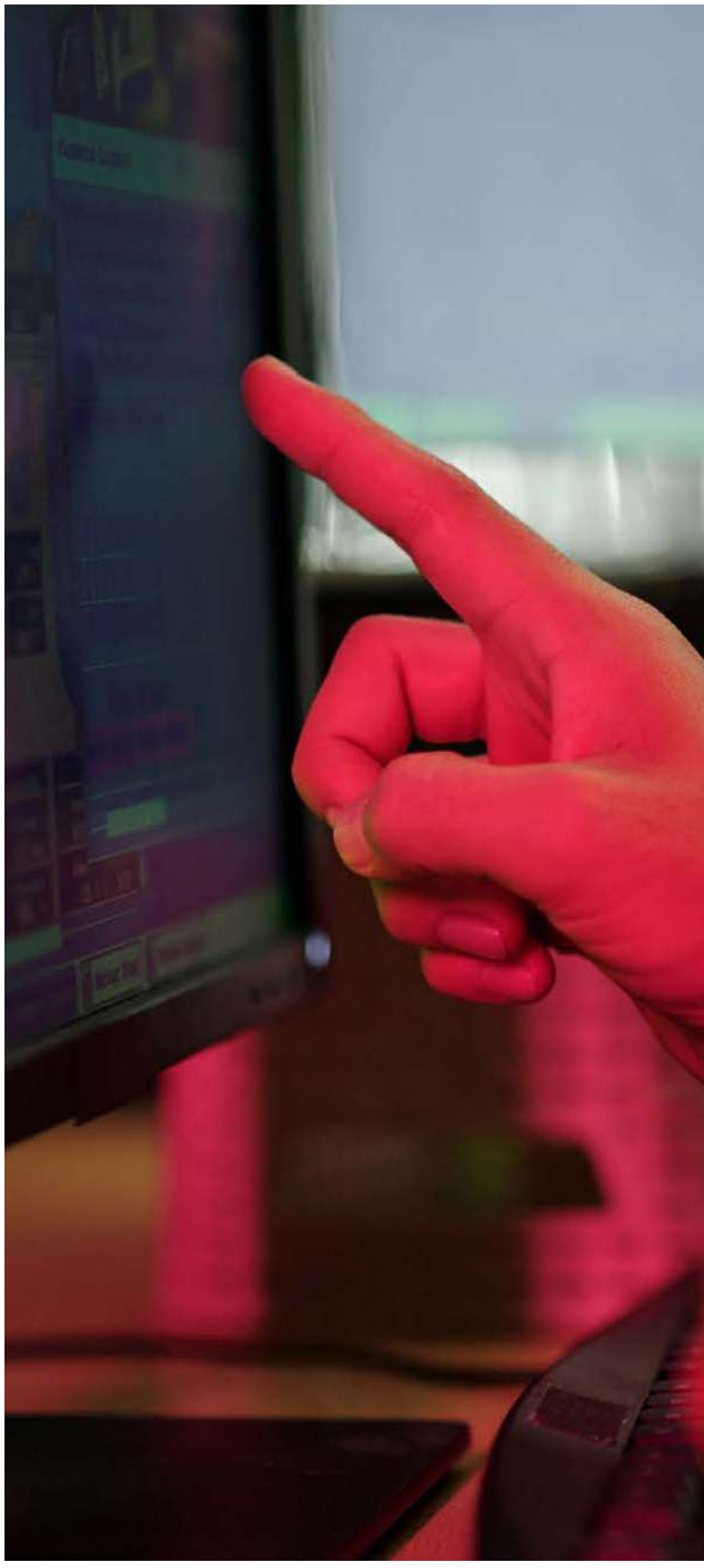
¿En qué áreas la seguridad empresarial está más consolidada y en qué otras sería necesario realizar una mayor toma de conciencia acompañada de más recursos (IA, IoT, Cloud, Trabajo Remoto…)?

(Jose Miguel Gómez-Casero Marichal) A día de hoy, la seguridad en el correo electrónico está madura en cuanto a sofisticación y detección estática (en algunos fabricantes, ofrecen detección incluso por comportamiento), aunque no se puede alcanzar el 100% de detección, desafortunadamente.

Veo frecuentemente a las organizaciones depender de los entornos cloud públicos más de lo que sus capacidades le permiten, en el contexto de ciberseguridad.

En estos momentos, ¿cuál dirías que es la principal amenaza a la que se enfrentan las empresas (ransomware, etc.) y cuál (si no coincide) es la más común o con la que los profesionales de la seguridad tenéis que trabajar más a menudo?

(Jose Miguel Gómez-Casero Marichal) Desde hace unos años los ransomware han abandonado su forma de malware, para evolucionar en organizaciones operadas por decenas/centenas de personas, donde **ya no puedes sentirte protegido por tener un antivirus, sino que los threat actors adaptan sus métodos cada semana para lograr sus objetivos.**
Esto hace que el ejercicio de mantenerse seguros en nuestras empresas se vuelva un reto constante.



En la actualidad los distintos fabricantes están posicionando nuevos enfoques como SASE, XDR, EDR… y seguro que no hay una única respuesta correcta… pero ¿por dónde debería empezar una empresa?

(Jose Miguel Gómez-Casero Marichal) **El objetivo final es proteger el entorno de nuestra organización, esto es, nuestros activos:** servidores, portátiles e identidades (cuentas de dominio, cuentas de servicio, etc.).

En este sentido, una empresa debe empezar siempre por el "endpoint", bien a través de un antivirus, un "Next Generation Antivirus", o dar el salto a tecnología EDR, en función del presupuesto del que se disponga.

Uno de los principales obstáculos a los que se enfrentan las empresas es la dificultad que tienen a la hora de atraer y sobre todo retener talento relacionado con la ciberseguridad. ¿A qué crees que es debido? Salario, estrés laboral, competitividad…

(Jose Miguel Gómez-Casero Marichal) Se trata de un mercado con mucha oferta, desde operativa nivel 1 de monitorización en un SOC hasta analista de malware y respuesta a incidentes.

No hay área donde no haga falta un experto en ciberseguridad (y experto también en el área en la que es necesario). Por encima de este punto, está el estrés laboral, ya que sobre los expertos en ciberseguridad recae la seguridad de las empresas, y todo lo que ello implica.

A menudo se dice que el eslabón más débil de una política de seguridad en la empresa lo constituyen los propios empleados. ¿Crees que se descuida la formación en seguridad informática en las empresas de nuestro país?

(Jose Miguel Gómez-Casero Marichal) Más que formación en ciberseguridad en sí, se trata de invertir en concienciación. **Los ejercicios de "Security Awareness" ayudan a las empresas a entrenar a sus empleados** para que, ante un ataque ejecutado vía ingeniería social, estén preparados y sepan qué hacer ante estas situaciones.

No se trata solo de realizar formaciones, sino también "simulacros" para ayudar a los empleados a estar familiarizados con los tipos de phishing que van a recibir, por ejemplo.

Por último, si tan solo pudieras hacer una recomendación sobre ciberseguridad a una empresa, ¿cuál sería?

(Jose Miguel Gómez-Casero Marichal) **Es importante concienciar a las empresas en invertir en ciberseguridad,** en lugar de asumir riesgos. La ciberseguridad no sale en el balance de cuentas, pero evita que los malos aparezcan en la zona de "gastos".

Fuente de información: muyseguridad.net