THREATQUOTIENT™

# ThreatQ para Entretenimiento y Videojuegos

Los sectores del entretenimiento y los videojuegos no están a salvo de los ciberataques. Según InfoSec Magazine, la exposición al público de la industria de los medios de comunicación es mayor a la de prácticamente cualquier otro sector. En estos sectores se incluye el cine, la televisión, la radio, las consolas de videojuegos, la prensa online e impresa, y se trata del ámbito que proporciona a las personas acceso a noticias e información del mundo exterior, además de satisfacer sus necesidades de entretenimiento[1]. De hecho, la enorme cantidad de usuarios es a menudo una de las razones por las que son víctimas.
Según Akamai, el sector de los videojuegos por sí solo experimentó un aumento del 167 % en el número de ciberataques en agosto de 2022 en comparación con el año anterior[2]. Además, los esfuerzos de fortalecimiento de la seguridad por parte de otros sectores como el de los servicios financieros y la Administración pública ha obligado a los ciberdelincuentes a recurrir a objetivos más fáciles como los sectores del entretenimiento y los videojuegos.

## DESAFÍOS PRINCIPALES

- **Menor nivel de concienciación en ciberseguridad de los jugadores**
- **Contenidos protegidos por derechos de autor como gran reclamo para los ciberdelincuentes**
- **Pérdidas económicas para las empresas y servidores inaccesibles para los usuarios**
- **Uso de compras dentro de aplicaciones o videojuegos vinculadas a credenciales bancarias**

### OBJETIVOS ATRACTIVOS

Los ciberdelincuentes se sienten atraídos por el sector [la industria del videojuego] como una superficie de amenaza en expansión, al considerar a los jugadores un grupo de víctimas potencialmente menos precavido[3]. Este sector no es el único. Todos los servicios de streaming son posiblemente demasiado relajados en sus hábitos, lo que aumenta las probabilidades de compromiso de su privacidad y seguridad informática[4].

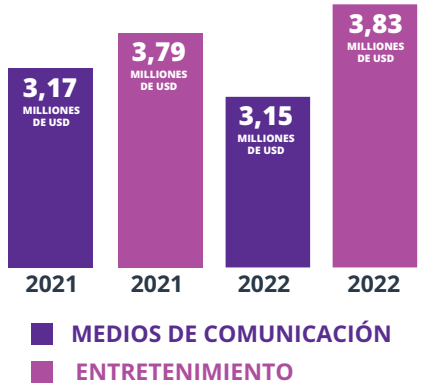
### RESPETO DE LAS MEJORES PRÁCTICAS

El crecimiento del sector de los medios de comunicación y el entretenimiento traerá consigo un aumento de la piratería, la extorsión, las interrupciones y el número de clientes afectados[5]. Por eso es cada vez más importante seguir las "mejores prácticas" de seguridad. Asegúrese de que su organización selecciona las herramientas adecuadas y que tienen una utilidad práctica.

### COMPROMISO Y PÉRDIDA

Los ataques distribuidos de denegación de servicio no siempre amenazan directamente la información personal. Lo más frecuente es que provoquen pérdidas financieras a las empresas de videojuegos y frustración a los jugadores que no pueden acceder a los servidores. Akamai documentó más de 3000 ataques de este tipo entre julio de 2019 y junio de 2020[6]. Esto también puede dar lugar al chantaje si determinados activos caen en las manos de los ciberdelincuentes[7].

### COSTE MEDIO DE UNA FUGA DE DATOS POR SECTOR




> Según Akamai, el sector de los videojuegos por sí solo experimentó un aumento del **167 %** en el número de ciberataques en agosto de 2022 en comparación con el año anterior.

## PLATAFORMA THREATQ

El modelo de datos flexible de ThreatQ permite a las empresas de entretenimiento y videojuegos la capacidad única de incorporar objetos personalizados en sus flujos de trabajo de análisis. Estas empresas no solo pueden utilizar ThreatQ para sus revisiones diarias, búsquedas de amenazas e investigaciones habituales, sino que también pueden ir un paso más allá y aprovechar los objetos personalizados para realizar un seguimiento de los usuarios que se aprovechan de trampas y exploits, software que explota sus videojuegos o servicios online y las relaciones entre ellos. En conjunto, esto permite a las empresas confiar en su nivel de seguridad, así como aumentar la longevidad de su base de usuarios, facilitando la mitigación de los exploits.

Las empresas de entretenimiento y videojuegos han utilizado objetos personalizados para rastrear videojuegos, códigos filtrados, desarrolladores de software cliente fraudulento, contraseñas, scripts, archivos multimedia y mucho más. ThreatQ ofrece a los analistas un único lugar en el que realizar un seguimiento de todos los elementos de contexto necesarios para actuar contra una amenaza. Entre desarrolladores, software, plataformas afectadas e incluso el hardware físico necesario para explotar un sistema, los elementos que hay que supervisar son muy numerosos. ThreatQ ofrece la capacidad única de satisfacer las necesidades de organizaciones que desean supervisar todos y cada uno de los detalles. Todo esto puede incorporarse sin problemas a la plataforma ThreatQ, permitiendo en última instancia a sus equipos de seguridad ofrecer una rentabilidad clara y oportuna.

## INTELIGENCIA SOBRE AMENAZAS LÍDER

La plataforma ThreatQ, que sirve de centro de operaciones de inteligencia para muchos sectores, agrega y combina datos estructurados y no estructurados procedentes de cualquier fuente, interna y externa. La automatización elimina las tareas repetitivas y laboriosas para que los analistas puedan centrarse en el trabajo estratégico y de mayor prioridad. La plataforma también ofrece flexibilidad para compartir rápidamente información curada sobre amenazas, avisos e informes con una amplia variedad de actores internos y externos, incluidos los sectores de infraestructuras críticas.

## CONSIGA MÁS CON THREATQ:

- **CONSOLIDE** todas las fuentes de información sobre amenazas y vulnerabilidades externas (por ejemplo, ME-ISAC) e internas (por ejemplo, SIEM Y EDR) en un repositorio central.
- **AUTOMATICE** las medidas de enriquecimiento en bloque, incluida la correlación de datos, la creación de relaciones y la incorporación de atributos adicionales y contexto para una comprensión más profunda de las amenazas y el análisis de tendencias.
- **ELIMINE** el ruido y explore fácilmente enormes cantidades de datos sobre amenazas para centrarse en los activos y vulnerabilidades críticos.
- **CALIFIQUE** las fuentes de inteligencia sobre amenazas y administre la caducidad automáticamente en función de sus requisitos para generar inteligencia de alta fidelidad.
- **PRIORICE** los datos en función de lo que sea más importante para las distintas partes interesadas y volver a hacerlo automáticamente a medida que se disponga de nuevos datos y conocimientos.
- **INTEGRE** con las herramientas y fuentes de información sobre amenazas existentes a través de una completa biblioteca de API y conectores personalizados.
- **COMPARTA** inteligencia y responda de inmediato a las solicitudes de inteligencia del SOC y otras entidades internas.
- **ACELERE EL ANÁLISIS** de los ataques y reduzca el tiempo de creación de informes y avisos de días a horas.

**Solicite una demostración en directo de la plataforma ThreatQ y de ThreatQ TDR Orchestrator en www.threatq.com/demo.**


1. https://www.infosecurity-magazine.com/news-features/cyber-attacks-media-industry/
2. https://www.infosecurity-magazine.com/news/gaming-sector-cyberattacks-167/
3. https://www.darkreading.com/threat-intelligence/cybersecurity-major-game-company-value-proposition
4. https://www.cisa.gov/sites/default/files/publications/gaming.pdf
5. https://www.verizon.com/business/resources/articles/s/preventing-cyber-attacks-in-the-entertainment-industry/
6. https://www.securedata.com/blog/gaming-industry-faces-growing-cyber-threats
7. https://www.forbes.com/sites/davidbalaban/2021/06/11/why-cyber-attacks-against-film-and-media-industries-are-escalating/?sh=214912226896


## ACERCA DE THREATQUOTIENT™

ThreatQuotient mejora las operaciones de seguridad fusionando diversas fuentes de datos, herramientas y equipos con el fin de agilizar la detección de amenazas y la respuesta. La plataforma de operaciones de seguridad de ThreatQuotient se basa en datos y ayuda a los equipos a priorizar los incidentes de seguridad, aplicar la automatización y colaborar en su resolución; permite tomar decisiones más fundamentadas; y optimiza el uso de recursos limitados integrando la tecnología y los procesos en un espacio de trabajo unificado. De esta forma se consigue reducir las detecciones irrelevantes, determinar qué amenazas son prioritarias y automatizar los procesos con datos precisos. Las funciones líderes en el sector de ThreatQuotient para la gestión de datos, la orquestación y la automatización cubren diferentes casos de uso, como la respuesta a incidentes, la caza de amenazas, el phishing dirigido, la clasificación de alertas y la priorización de vulnerabilidades, y también pueden servir como plataforma de inteligencia sobre amenazas. ThreatQuotient tiene su sede central en Virginia del Norte y centros de operaciones internacionales en Europa, Asia Pacífico y Oriente Medio-Norte de África. Para obtener más información, visite www.threatquotient.com.

TQ-IDB03-0823-01

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885