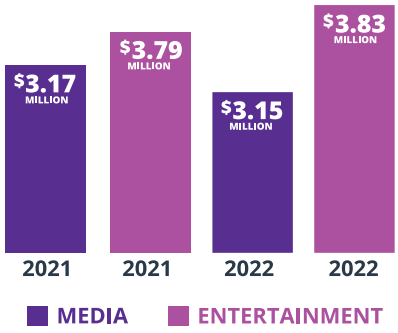
THREATQUOTIENT™

ThreatQ for Entertainment & Gaming

The Entertainment and Gaming industry is not safe from cyber attacks. According to InfoSec Magazine, the media industry is more visible to the public than virtually any other sector. Encompassing film, television, radio, gaming consoles, online and print, it is the arena that provides people with access to news and insights into the outside world, as well as fulfilling people's entertainment needs.[1] In fact, they fall victim quite often due to the amount of users. According to Akamai, the gaming sector alone was faced with an increase of 167% of cyber-attacks in August of 2022 compared to the previous year.[2] Also, with other sectors like financial services and government building stronger security operations for protection against cyber attacks, threat actors are turning to an easier target like the Entertainment and Gaming industries.

AVERAGE COST OF A DATA BREACH BY INDUSTRY



KEY CHALLENGES

- **Gamers are less cautious about cybersecurity**
- **Copyrighted content is a big lure for threat actors**
- **Financial loss for companies and inaccessible servers for users**
- **Using in-app or in-game purchases linked to banking credentials**

> According to Akamai, the gaming sector alone was faced with an increase of **167%** of cyber-attacks in August of 2022 compared to the previous year.

ATTRACTIVE TARGETS

Cybercriminals are drawn to it [the video game industry] as an expanding threat surface, seeing players as a potentially less cautious group of victims.[3] The gaming industry is not alone, all online streaming services are potentially too relaxed in their habits with the opportunity for compromise of their privacy and computer security.[4]

FOLLOWING BEST PRACTICES

As the media and entertainment sector continues to grow, piracy, extortion, disruption and the targeting of customers is only likely to increase.[5] This is why the importance of following security "best practices" are increasingly important. Make sure that your organization selects the right tools and makes them actionable.

COMPROMISE AND LOSS

Distributed denial of service attacks don't always directly threaten personal information. More often, they cause financial losses for gaming companies and frustration for gamers who can't access servers. Akamai documented more than 3,000 such attacks from July 2019 to June 2020.[6] This can also lead to blackmail if the wrong assets fall into the wrong hands of cyber criminals.[7]

THREATQ PLATFORM

The ThreatQ flexible data model allows entertainment and gaming companies the unique ability to incorporate custom objects into their analyst workflows. Not only can these companies use ThreatQ for their typical day-to-day reviews, threat hunts, and investigations; they can also take it a step further to leverage custom objects, tracking users who take advantage of cheats & exploits, software that exploits their games or online services, and the relationships between. All together, this gives these companies confidence in their security posture as well as increasing the longevity of their user-base by facilitating the mitigation of exploits.

Entertainment and gaming companies have utilized custom objects to track games, leaked codes, cheat client software developers, passwords, scripts, media source files and more. ThreatQ gives analysts a single-place where they can track all the pieces of context required to take action against a threat actor. There's a lot to track between the developers, the software, the affected platforms, and even the physical hardware required to exploit a system. ThreatQ offers the unique ability to cater to organizations wanting to track each and every bit of detail along the way. All of this can be seamlessly incorporated into the ThreatQ Platform, ultimately, allowing your security teams to provide a clear and timely ROI.

CREATING A LEADING THREAT INTELLIGENCE OPERATION

Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to quickly share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including critical infrastructure sectors.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external (e.g., ME-ISAC) and internal (e.g., SIEM, EDR) threat intelligence and vulnerability data in a central repository
- **AUTOMATE** enrichment actions in bulk, including correlating data, building relationships, and adding more attributes and context for a deeper understanding of threats and trend analysis
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities
- **SCORE** threat intelligence sources and manage expiration automatically based on your requirements to produce high-fidelity intelligence
- **PRIORITIZE** data based on what matters most for different stakeholders and reprioritize automatically as new data and learnings are available
- **INTEGRATE** with existing tools and threat intelligence sources via a comprehensive library of APIs and custom connectors
- **SHARE** intelligence and respond to requests for intelligence from the SOC and other internal entities right away
- **ACCELERATE ANALYSIS** of attacks and reduce time to create reports and advisories from days to hours

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at 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

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit 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