



# iThreat LifeCycle

PROTECT YOUR INTELLECTUAL PROPERTY FROM CONCEPT TO COMMERCE

The window for an entertainment company to make a profitable return on movies and video games is shorter than it ever has been. Digital downloads and other home offerings have reduced the window in which the content creator or distributor can get return on investment. This can be massively affected if a leak, or early release of information or materials associated with the IP, occurs online ahead of “your window”.

The entertainment space is no stranger to these “*insider-leaks*” and is a popular target for fans hungry for information. Knowledgeable insiders are often happy to “share” when they think they can “be anonymous” online.

iThreat has long provided Threat Intelligence Programs to the Entertainment industry under the “LifeCycle Monitoring” name, specifically tailored to uncovering online leaks of intellectual property through the monitoring of social media and expansive online communities. We are known to be the first company to provide this kind of service to any Hollywood feature, and have seen many competitors try to emulate the service with low success. “**iThreat LifeCycle**” can be deployed efficiently & cost effectively to ensure that you are the first to know where people are leaking early information online and beyond.

The added value iThreat’s “**KnowledgeBase**” model offers is one of both scale and heuristics. All data captured relevant to our program for your company is parsed, modeled, and structured for continued cross-reference and relevance detection. This allows for predictive and prescriptive programs that continue to improve as engagements grow and evolve through various threat vectors.

iThreat takes Signal Detection and turns that into Signal Intelligence. Our programs focus on finding the relevant signal in the noise. Many other programs may help you find the signal. iThreat focuses on finding the signal, managing the interpretation, correlation and impact to your organization through our Threat Intelligence Program.



---

## Monitoring Vectors for a Successful LifeCycle Program

- A: Information Leak Monitoring:** In addition to keyword-based social media monitoring, iThreat will enumerate and monitor for information leaks on fan sites, discussion forums, forum threads, industry news sources, key threat community leaders/influencers, social media accounts, and insider social media activity. Information leaks may include premature public mention of plot details, characters, title codenames, unannounced actors, key props, filming locations, script leaks, and similar information. Additional specific forms of information leak monitoring iThreat will employ are described below.
- B: Phishing/Fraud Domain Monitoring:** iThreat will leverage its [CyberToolBelt.com](https://www.CyberToolBelt.com) platform and data to monitor for registration of domain names which include keywords associated with the title, the Client, title production entities, and key persons associated with the title.
- C: Merchandise Leak Monitoring:** Information associated with titles is occasionally exposed due to leaks of merchandise associated with the title or information about the merchandise, to include toys, books, costumes, and similar items.
- D: Theft Detection:** iThreat monitors popular Internet marketplaces for unauthorized sales of items associated with the title.
- E: Darknet Monitoring:** iThreat maintains a database of known .onion (Tor Network obfuscated) websites, to include site title, .onion URL, partial site text content, and meta keywords. Known and newly detected .onion sites are periodically scanned for known information associated with Client title and alerts are provided should iThreat detect any matches.
- F: Paste Site Monitoring:** iThreat monitors to the extent possible known Paste sites (primarily Pastebin) commonly used by threat actors to post confidential information. iThreat monitoring detects known information associated with Client title and alerts are provided should iThreat detect any matches.
- G: Mobile iDupeCheck and iDupeCheck:** Monitoring for infringing or unauthorized recordings and digital copies of Client title and for the presence of Client mobile applications in unauthorized app repositories is provided. Apps are often modified by threat actors for operation on jailbroken or insecure mobile devices, or modified for other malicious purposes.
- H: Location Threat Monitoring:** iThreat will employ geo-filtered social media monitoring surrounding known production locations and screening/festival locations.
- I: General Infringement Threat Intelligence:** iThreat may provide general infringement threat intelligence regarding vulnerabilities, methods, infrastructure, and tools leveraged by threat actors to obtain, distribute, and consume the earliest instances of unauthorized or infringing content as this intelligence may pertain to Client title.
- J: Disruptive Threat Monitoring:** iThreat will identify title topics and themes likely to attract disruptive activist and interest group responses. iThreat will also provide activist threat assessments associated with known filming locations. Additionally, iThreat will monitor for threats incited by, or threats toward, key actors, directors, and producers associated with the title.

---

## About iThreat

iThreat builds, augments, and supports Threat Intelligence Programs that enable customers to protect their people, assets, and brands with real-time, predictive, actionable intelligence. Founded in 1997, iThreat has been on the leading edge of threat intelligence since the early days of the Internet. iThreat uses a cloud-based software platform and our investigative and technology expertise to generate real-time, prescriptive, and actionable intelligence programs. iThreat is a fully GDPR compliant company that is focused on commercial markets, with unique expertise in the technology, healthcare, and entertainment verticals.

*Let us help you structure a Threat Intelligence Program that is right for you.*

Contact us for more information: [www.ithreat.com](https://www.ithreat.com)

Headquarters: 317 George Street, New Brunswick, NJ 08901

Mailing Address: PO Box 276, New Brunswick, NJ 08903

+1 609-806-5000 | [sales@ithreat.com](mailto:sales@ithreat.com)

