CASE STUDY

Leading Media and Entertainment Company Protects Its Intellectual Property and Manages Risk with Recorded Future®

A leader in media and entertainment relies on Recorded Future to identify and remediate data leaks and assess its risk posture

Use Case:

Protect their brand and its assets from threats that could result in intellectual property loss or reputational damage.

Challenge:

Lack of real-time visibility or context to help teams proactively address risks such as vendor risk, intellectual property leakage, and device vulnerabilities.

Solution:

The Recorded Future Intelligence Cloud, including:

- Brand Intelligence
- Vulnerability Intelligence
- Threat Intelligence
- Third-Party Intelligence
- SecOps Intelligence

Outcomes:

- Identify and stop typosquatting and active phishing campaign
- Identify and shut down malicious infrastructure targeting high value assets
- Address high-risk vulnerabilities that can lead to data loss
- Use Recorded Future to obtain insights into third-party risk
- Leverage Recorded Future to measure progress against intelligence goals

In the media and entertainment industry, data leaks about a big product release can severely impact both revenue and customer perceptions. The risk of data loss is further heightened by the scope of the projects and the sheer quantity of third-party contributors who work on any given product. That's why a top media and entertainment company uses Recorded Future to maintain visibility into its rapidly changing threat landscape and to mitigate risk proactively.

"Third-party risk is a huge element in our value chain. At the highest levels of the company, my job is about risk awareness and helping executives understand the big picture behind an incident or a string of incidents, or what we're seeing being reported in the news and how that relates to what we're seeing internally," says the company's Cyber Threat Intelligence Manager.

Looking for Visibility

The intelligence team hasn't always had the visibility it needed to provide the insights business leaders are looking for. "If an executive asked me to track a threat or keep a pulse on whether information was getting leaked, I thought 'it would be great if we could do that, but we couldn't.' But now, with Recorded Future, we can. Recorded Future helps our teams contextualize and articulate risks in a way that is digestible and relevant to the business," says the Cyber Threat Intelligence Manager.

The media and entertainment company went through a methodical evaluation process to select an intelligence provider, and saw Recorded Future's value right away. "During the evaluation stage, the Recorded Future team did a really outstanding job getting to know us and our concerns, and they set up the platform to produce automated high-value alerting during the proof of concept. They set up domain monitoring logic that identified phishing targeting our assets," says the Cyber Threat Intelligence Manager.

Their intelligence team was also pleased with the Recorded Future Intelligence Platform; "During the trial we were really impressed with the way the platform is organized around intelligence requirements and the ability to track how what we're doing from an alerting standpoint flows up into a broader set of requirements that the team is working on," says the Cyber Threat Intelligence Manager. "That's something that really differentiates Recorded Future, and it helps our teams organize and understand what they're looking for, what data they have, and where the gaps are."

The coverage and visibility provided by Recorded Future has enabled the media and entertainment company to identify and mitigate threats to its brand. "I'm a huge fan of Recorded Future's Brand Intelligence. It has enabled us to discover threats before they hit our network," says the Cyber Threat Intelligence Manager. With Brand Intelligence, the team also discovered and shut down malicious infrastructure impersonating the company and executing phishing attacks targeting high value assets.

Protecting Intellectual Property and Managing Vendor Risk

The security team also uses Recorded Future to quickly identify information leaks before big product launches, as well as, monitor for post-launch data abuse. "We are able to identify new domains containing stolen assets as they are being created. We then package up the research, and send it to our internal team that actions takedowns on them," says the Cyber Threat Intelligence Manager.

Recorded Future's Third-Party Intelligence delivers additional value. "There's a lot of executive anxiety about product details being leaked before they are released because many small vendors and contractors are involved in product launches and directly handle our highest value data," says the Cyber Threat Intelligence Manager. "Third-Party Intelligence provides a different perspective on the profile of a vendor that we're working with. We can see past incidents that they've had, and spot check their security hygiene in real-time. It helps to give the risk assessor a different perspective, and some additional questions, that they can probe into with their points of contact at the vendor."

Taking intelligence further, the team also uses Recorded Future to research potential technology vulnerabilities that third parties inadvertently introduce to projects. "The ability to identify vulnerabilities in niche technologies used in the industry has also been of high value to us," says the Cyber Threat Intelligence Manager. For example, project teams sometimes use very specific devices. The intelligence team uses Recorded Future to research those devices for vulnerabilities.

"If a device vulnerability is targeted by ransomware actors, the alert is passed to the technology teams to let them know that not only is there a vulnerability, but it's being targeted by ransomware, and they need to take the necessary steps to discontinue the use of that device," says the Cyber Threat Intelligence Manager.

Alerts are tracked in Recorded Future, enabling the intelligence team to see improvements in the company's risk posture. "It's very, very easy to name alerts, associate them with intelligence goals in a way that is rational, so we can measure what we're doing and how we're doing it," says the Cyber Threat Intelligence Manager.

The team's work has earned it some notoriety. When business leaders want to know about the latest security issue making news headlines, the intelligence team is known for having answers. "Being able to confidently say we understand how a threat to our industry impacts us is very valuable, and our team has become known for having this information. Now, thanks to Recorded Future, people come to us looking for validation that the problem they're dealing with is covered."