·|:|·· Recorded Future

From Flying Blind to Clear Skies:
How One Airline Uses Threat Intelligence to Better Detect Threats and Protect People's Lives

When it comes to cybersecurity, airlines have a ton of information to protect — credit card numbers, names, dates of birth, passport information, flight information, and more. For this major airline, however, even more important than protecting information and preventing breaches is protecting people's lives.

To track and understand potential threats, this airline employed several threat intelligence analysts, but with the amount of data they needed to research, they couldn't risk things being missed. Their process, which used to take hours upon hours of manual research, is now much more sophisticated and efficient, allowing this airline's team to feel confident that they're helping to protect the organization and its passengers from threats.

Using Threat Intelligence for More Than Cybersecurity

Many companies look for threat intelligence to help with things like understanding the types of attacks that are trending in their industry, preventing hackers from stealing personal information, or protecting their brand reputation. In talking about her organization's main threat intelligence priorities, the leader of the threat intelligence team says, "Before information getting stolen, before breaches, if there is something that is actually going to impact lives, that is of the utmost importance."

One major capability her team needed was access to a broad range of sources, including the dark web, to help them surface relevant information, like violent sentiments against the airline, bomb threats, and more. "We're looking at a world of things from physical security to cybersecurity," the team lead says, "and we needed a company like Recorded Future to go through the masses and masses of data and pull this in for us."

> "Before information getting stolen, before breaches, if there is something that is actually going to impact lives, that is of the utmost importance."

Relevant Alerts Surfaced Instantly

With manual threat intelligence collection, the best you can do is search for as many sources as possible, hoping to find relevant, actionable data. The challenge with this approach, as this airline quickly realized, is that it takes far too long to just scratch the surface of data that is out there, making it too easy to miss something critical. With Recorded Future, the team lead loves that her people wake up to the different things that Recorded Future has found for us overnight, whether it be exposed credentials, or some kind of attack, or bomb threat."

THE CHALLENGE
- Needed broader source coverage
- Spent too much time manually researching
- Used multiple disparate sources of intelligence
- Had a vast amount of attack vectors to watch

THE SOLUTION
- Alerts automatically surfaced in real time
- Aggregation of internal and external threat intelligence in one central location
- Intelligence integrated seamlessly into existing security workflows

THE RESULTS
- More confident coverage of potential threats
- Less time spent manually contextualizing alerts
- Ability to respond faster to incidents
- Better visibility and sharing of intelligence

And when they do need to look into something, rather than spending time manually researching, they can use Recorded Future to pull up the relevant data instantly. "The context in Recorded Future is unparalleled. We can look up something like an IP address and all of a sudden get this world of information," says the threat intelligence lead. Through the speed and scale of automated collection and the ability to tailor alerts to its specific industry, technologies, and use cases, the airline's team had insight into more than ever before; and without the lag time of human research, they were able to prioritize and respond to these alerts faster.

> "The context in Recorded Future is unparalleled. We can look up something like an IP address and all of a sudden get this world of information."

The Power of an All-in-One Solution

The airline's original strategy for building a threat intelligence practice included acquiring both a threat intelligence provider and a separate threat intelligence platform (TIP). After evaluating many vendors, ultimately Recorded Future and a TIP vendor were selected and integrated. Over time, this airline realized the capabilities that it was depending on the TIP for — mainly integrating A-ISAC (Aviation ISAC) data and other proprietary sources into its threat intelligence — were available directly in the Recorded Future solution through a product called Fusion.

Having all threat intelligence capabilities available in a single solution has helped the airline create a single source of truth for all its intelligence, collaborate more effectively, and react faster. Also, it's found that working with a single vendor simplifies and speeds up its day-to-day operations. On working with Recorded Future, the team lead says, "It has been really just a wonderful customer experience."

Threat Intelligence for the Whole Organization

The airline integrates Recorded Future intelligence into its existing workflows, like those in its SIEM, and has future plans for integrations with endpoint and incident response solutions. Recorded Future brings value to more than just its threat intelligence team — it helps the entire organization. "We share the information that we get from Recorded Future with multiple teams — that includes our cyber operations center, our monitor and detection team, as well as our vulnerability management team, our risk compliance team, and our security awareness team that does training and education for our employees. We're sending information to corporate security, you name it," the team leader says. Even its executive team has benefited from Recorded Future with finished intelligence reports that make it easy to digest and understand specific issues.

> "We share the information that we get from Recorded Future with multiple teams."

Conclusion

As the airline has found, a security strategy fueled by intelligence is very effective for understanding, preventing, and responding to threats. And when a company, like this airline, is responsible for protecting people's lives as well as their information, an intelligence-driven approach is paramount.

Find out more.   (855) 476-9728
www.recordedfuture.com/demo

Recorded Future