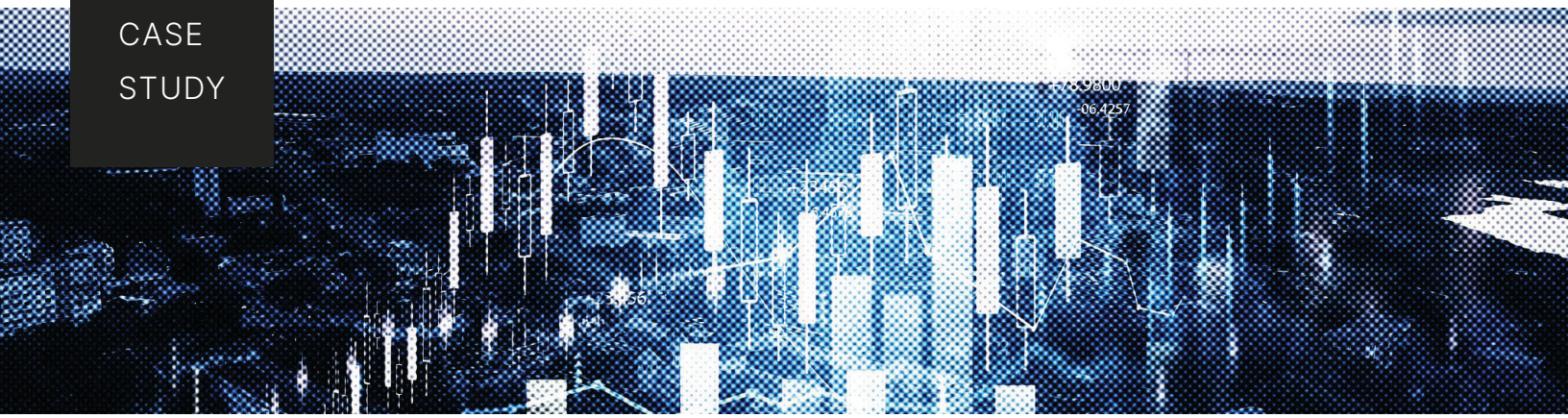
Recorded Future®

CASE STUDY



Kyriba Relies on Threat Intelligence to Grow and Protect Their Business

Global financial services leader uses Recorded Future to secure customer data and core business Intellectual Property

Kyriba

Goal:

Prioritizing cyber risk across the fast-changing financial services threat landscape

Challenge:

Understanding, predicting, and communicating which threats pose the greatest risk to customer data, intellectual property (IP), and the company brand.

Solution:

The Recorded Future Intelligence Cloud featuring:

- Threat Intelligence
- Brand Intelligence
- SecOps Intelligence
- Recorded Future for Splunk Integration
- Vulnerability Intelligence
- Identity Intelligence

Outcomes:

- Emerging threats prioritized and contextualized to implement effective protection
- Kyriba brand protected from digital risks such as phishing and domain abuse
- Streamlined and automated security workflows within Splunk
- Proactive reporting of risk to Kyriba leadership and other stakeholders

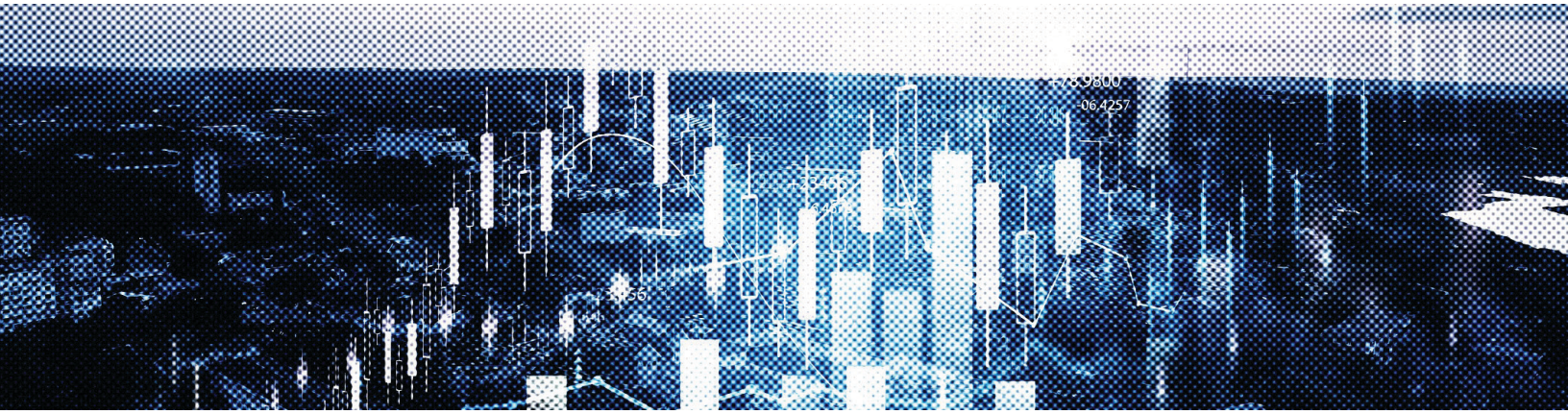
Financial services institutions build some of the world's strongest cyber defenses, but threat actors still try to follow the money. A global innovator at the forefront of Enterprise Liquidity Performance (ELP), Kyriba's priorities for cybersecurity include protecting its clients' financial data and operations against ransomware, exfiltration, downtime, and revenue loss caused by cyberattacks.

Serving more than 2,500 clients in 100 countries, Kyriba takes its role as 'guardian of customer data' seriously. "Data makes companies these days — it's the data you have and how you use it that provides real value to customers," says Kyle Abbey, Senior Manager, Cyber Security at Kyriba, provider of cloud treasury and financial services for more than 20 years. "We need to make sure the customer data we possess stays protected."

Cybersecurity engineers also worry about Kyriba's intellectual property (IP) being stolen. To predict and mitigate risk from today's volatile threat landscape, the provider's cybersecurity team sought to leverage threat intelligence from the beginning.

"Back when our security organization was still new, threat intelligence was a capability we knew we wanted to purchase," says Kyriba Senior Manager, Cyber Security Kyle Abbey. "We were doing some Open Source intelligence, gathering information where we could, but we knew there were better features and platforms out there."

To find its ideal solution, cybersecurity leaders commissioned a bake-off to compare leading threat intelligence solutions. After close evaluation, Recorded Future's Intelligence Cloud emerged as the clear winner.



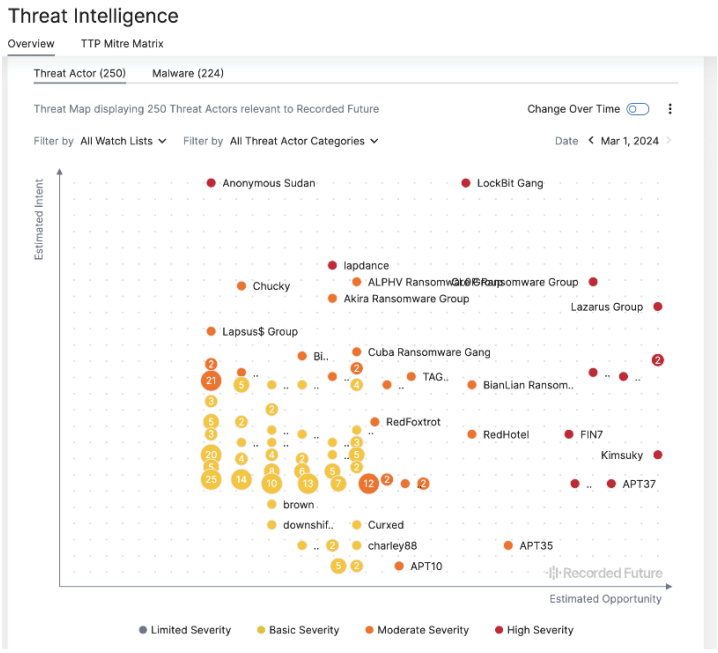
> **Recorded Future adds context that explains why our team might be focused on LockBit, one of our biggest adversaries, instead of something Forbes magazine is talking about that doesn't really impact our industry."**
>
> *Alex Minster,*
> *Security Engineer, Kyriba*

Recorded Future Delivers a Prioritized View of Risk

Kyriba relies on Recorded Future to gain a deeper understanding of which threat actors have an intent — and opportunity — to target their organization. Intelligence generated by the Recorded Future platform stands apart from other sources as a reliable, up-to-the-minute single source of truth.

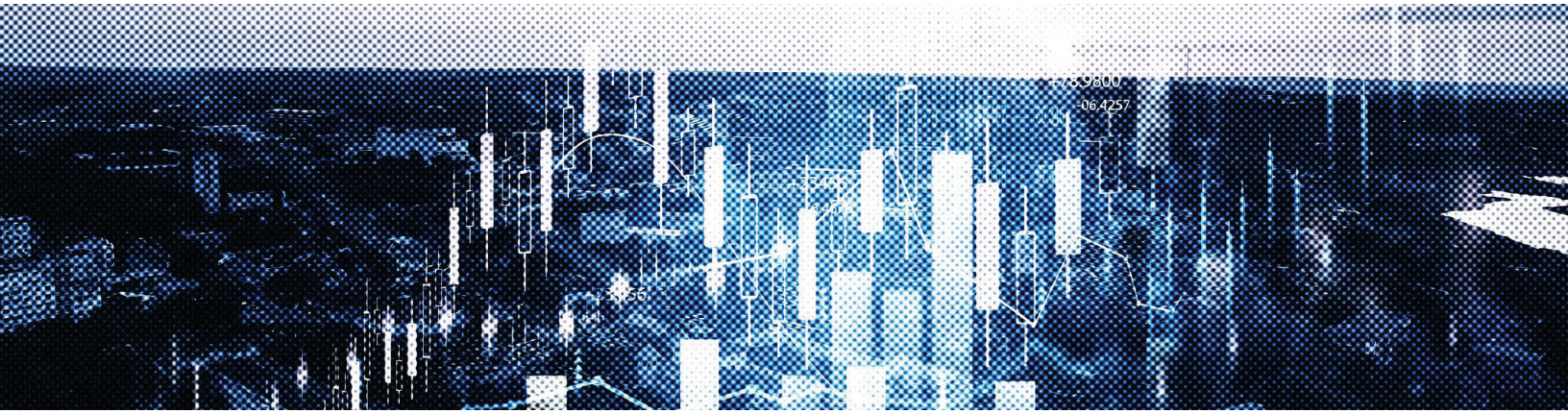
"Whenever something breaks in the information security realm, there's always a lot of chatter back and forth," says Security Engineer Alex Minster. "Recorded Future distinguishes itself by filtering out the relevant information from the noise. The intelligence they send out is something we can take as factual, deliver to the team, and provide to upper management as well."

Security engineers highlight Recorded Future's Threat Map in their regular reports on news impacting the financial services industry. The maps provide an at-a-glance visualization of the top threats to the business and easily enable the Kyriba team to further investigate new and emerging threats.



The Kyriba cybersecurity team uses the Recorded Future threat map to understand which threat actors are likely to target their organization so they can proactively tune controls to eliminate risk.

"There are always lots of interesting stories about threat actors targeting the financial industry, but they don't all directly impact Kyriba," Minster explains. "Recorded Future adds context that explains why our team might be focused on LockBit, one of our biggest adversaries, instead of something Forbes magazine is talking about that doesn't really impact our industry."



Prioritization makes the team look 'prophetic'

Honing in on the most relevant threats helps security analysts predict and forewarn company leaders of threats brewing in the wild. Minster credits Recorded Future's proactive intelligence with highlighting new cyber threats on the front end and helping to flag dangerous exposures like hijacked domains and stolen credentials on the back end.

"Threat intelligence from Recorded Future makes our team look prophetic," Minster says. "We're able to say, 'here's something we need to be worrying about so let's raise awareness around that,' and sure enough, it starts to land on our shores a month or so later. It's been a great boost to our organization to have Recorded Future provide that early 'heads up' so we can get out in front when something bubbles up."

Actionable insights protect the brand

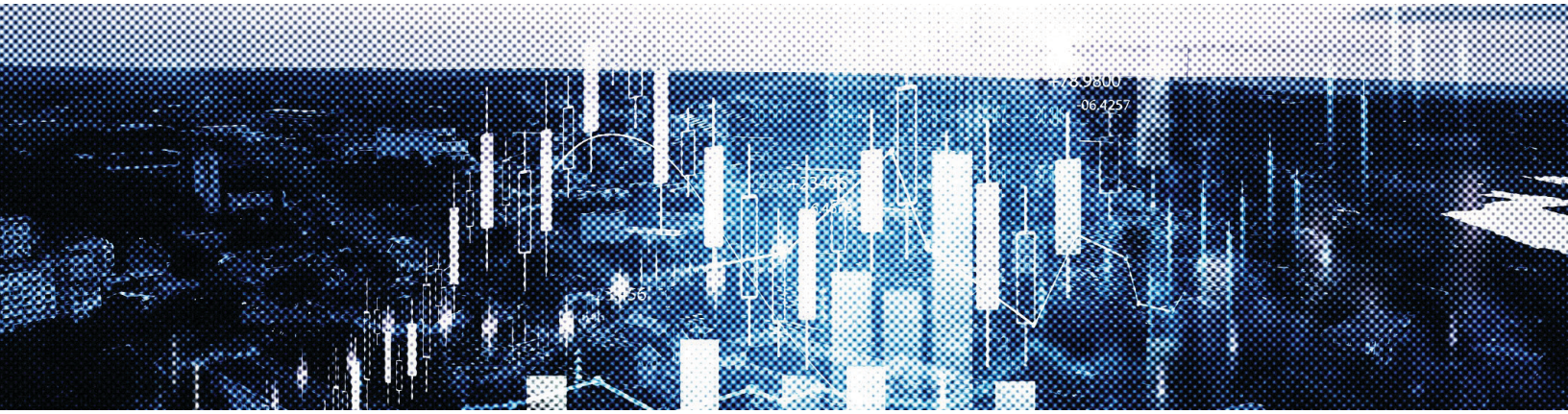
Along with preventing or triaging high-severity threats quickly, the team relies on Recorded Future's Brand Intelligence to protect Kyriba's brand reputation and bottom line. "If someone were able to break through and steal or replicate our formula, they might try to offer a similar service at a lower price to draw customers away," Abbey says. "That type of thing is hard to come back from."

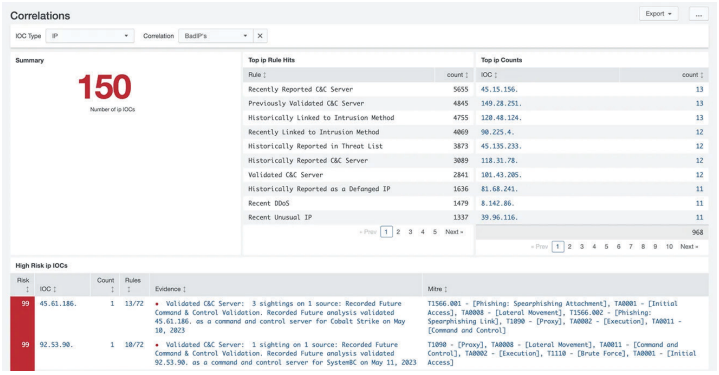
Recorded Future Brand Intelligence spots subtle risk indicators from popular cybercriminal techniques such as phishing, domain abuse, spoofing IP addresses, and standing up fraudulent websites or pages related to phishing and ransomware campaigns. "A sweep through Recorded Future might show a series of events that could be the start of someone staging malicious sites," Minster explains. "Brand intelligence provides the context we need to determine whether something sketchy that pops up actually indicates domain abuse or is just part of a block of legitimate domains."

Intelligence Makes Security Investments Work Smarter

Recorded Future integrates with Kyriba's existing solutions to streamline their security workflows and scale investigations. For example, close integration with Splunk automates the process of correlating real-time threat intelligence against massive amounts of data collected from security tools.

Noting that there's "rarely a shortage of threats these days," Abbey says the team funnels and aggregates logs from other security and monitoring tools within Splunk. Using Recorded Future to prioritize and contextualize security events within Splunk reduces the time it takes to understand which threats represent the greatest risk to Kyriba.





Recorded Future provides analysts working within Splunk with enhanced context to identify and prioritize risk, and context to improve alert investigation

"We use the correlation dashboards in Recorded Future's app for Splunk to pull up what's relevant and sort by severity," the security engineer explains. "Surfacing one IP among billions is hard so being able to sort according to risk and work our way down the list definitely helps us start triaging faster."

Recorded Future helps put defenses to the test

The Kyriba team also pairs insights from Recorded Future with breach and attack simulation (BAS) tools to assess and bolster defenses. The platform surfaces high-risk cyber criminals and active threats that help the team conduct simulated attacks.

Recorded Future data also helps explain and justify testing that might otherwise seem intrusive. "Someone might ask why we're doing things that light up their dashboards," Minster says. "With Recorded Future we're able to show that there's something new out there that impacts our industry, and that we need to make sure it doesn't come through our defenses."

Documentation demonstrates the value of intelligence

Security Engineer Alex Minster credits Recorded Future's publicly-available Intelligence Handbook with making it easy to articulate the value of world-class threat intelligence to partners and colleagues. "There are all sorts of great things to reference and show how companies can squeeze more value out of existing investments," Minster concludes. "The guides say everything I want to say about why threat intelligence is so important. That's another thing we really like from Recorded Future."

ABOUT RECORDED FUTURE

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.