CASE STUDY

Lean, nimble security team scales to enterprise-grade

Fintech innovator differentiates its cybersecurity program with the Respond Analyst

"In the financial services industry, cybersecurity is of absolute importance because our client companies wouldn't have any confidence in us if we didn't have a very strong information security program," explains Eric Adams, Chief Information Security Officer at Kyriba. "Proving that we conform to strict security standards is something we take extremely seriously in our company."

Though less than two decades old, **Kyriba**, a global treasury management solution provider, has already won multiple awards for the fully virtualized and cloud-based cash management solutions it delivers to more than 2,000 clients around the world.

Kyriba's clients rely on its innovative solutions to optimize cash and liquidity management; track financial transactions; monitor, control, and screen payments; detect fraudulent or suspicious activities; and match accounting balances from the general ledger against bank actuals. As a result, Kyriba must conform to some of the world's most stringent regulatory compliance requirements, including GDPR, France's even stricter CNIL data privacy law, and the rigorous data security standards that must be met in order to establish SWIFT connectivity with banks and other financial transaction processors. Kyriba also meets SOC 1 and SOC 2 Type II auditory reporting standards. Some applications already meet the ISO 27001 standard, and Kyriba expects that its full solution portfolio will do so by next year.

Kyriba's nimble team gains formidable capabilities with decision automation

To protect its multinational cloud-based infrastructure, Kyriba built its own private, dedicated cyber defense facility in San Diego. Together with a lean but agile security team, Kevin Bailey, Director of the Cyber Defense Center at Kyriba, was tasked with building a cybersecurity program that would span the globe and meet the financial industry's strictest standards with less staffing. Bailey knew he would need to leverage the power and scalability of the cloud, and rely on intelligent automation to monitor and triage the endless stream of security data.

"We knew we'd never be able to achieve the level of security we wanted—to maintain an extremely safe environment for everyone doing business with our systems—without finding this balance between humans and machines," says Adams.

Kyriba decided to implement the Respond Analyst because of its unique capabilities, and because IT leaders were impressed with the software's performance in proof-of-concept testing. The distinctly human qualities possessed by the Respond Analyst's designers—deep industry knowledge and long-term experience—stood out. "The Respond Analyst's creators are some of the most knowledgeable veterans in the entire security space," says Bailey. "With the Respond Analyst, we're basically getting their experience in a box."

kyriba

Chief Information Security Officer:
Eric Adams

Cyber Defense Center Director:
Kevin Bailey

Industry: Technology

The Tech Environment:

Coverage Data: Multiple office locations worldwide; 2000 client companies

Size of Team: Smaller nimble team

Environment: Cloud-to-Cloud AWS instance Splunk connected to the Respond Analyst AWS instance

Tools: Palo Alto Networks IDS/IPS; Palo Alto Networks URL filtering; McAfee Endpoint Antivirus; Carbon Black Advanced Endpoint Protection Platform.

Number of Security Events Before:
28 billion/3 month period

> *"The more data we can throw at it, the better. And we also liked the idea of the software's consistent performance. I know that the Respond Analyst is looking at these events the same way every single time, in accordance with some of the best thinking in the industry."*

Kyriba takes advantage of the Respond Analyst's scalability and consistency. "The more data we throw at it, the better," says Bailey. "And we also like the idea of the software's consistent performance. I know that the Respond Analyst is looking at these events the same way every single time, in accordance with the best thinking in the industry."

Amplify existing security investments

Kyriba, a Software-as-a-Service (SaaS), always looks to the cloud first when seeking to meet its own technology needs. One of the key advantages of Respond's solution was the ease with which it integrated with Kyriba's existing cloud-based security stack. All logs from their Palo Alto Networks intrusion detection system/intrusion prevention system (IDS/IPS) and URL filtering platform, as well as their McAfee endpoint antivirus solution, were being aggregated and fed into their Splunk System Information and Event Management (SIEM) tool. The Respond Analyst readily integrated into this security architecture without straining system resources or requiring excess overhead.

The fact that Splunk and the Respond Analyst can communicate via APIs makes their integration simple. "I don't have to burden my engineering team or my DevOps team or my IT team to make configuration changes to infrastructures to facilitate getting logs to Respond," says Bailey. "Adding new data sources requires nothing more than a simple configuration change on the Analyst."

Kyriba has installed the Respond Analyst in its AWS instance, and Splunk is hosted in Splunk's AWS instance. This means that all data travels directly from cloud to cloud. It's an ideal setup for a cloud-first organization, and particularly one that's so centrally concerned about security. "If you'd gone through some of the compliance programs that we've been through as a team, you'd know that you can make a cloud solution a lot more secure than a traditional on-prem system," says Adams.

Time-to-value: very quick

The deployment process was rapid and relatively seamless. Kyriba's team began directing data sources to the Respond Analyst in February of 2019, and went live the following month. To test their new 'automated' co-worker, the security team members conducted an internal red team exercise. "We wanted to see if Respond would pick up on the "attack," and it did. From that point on, we felt pretty confident that the things it was going to escalate were all things that we legitimately needed to take a second look at," says Bailey.

The Respond Analyst proved able to identify vulnerability scanners and device misconfigurations without any prior knowledge of the environment. "That's essentially the same thing an attacker would do," explains Bailey. "Right away it helped us uncover some of the skeletons that were in our closet."

Security team energized and happy

Since joining Kyriba's security team, the Respond Analyst has proven its value time and time again. Within any given 90-day window, Splunk will index approximately 28 billion events. Before the Respond Analyst's implementation, the team wasn't able to examine more than a tiny fraction of them. "Today we have an overarching sense of confidence in the fact that these events are all being looked at. We don't have any fears that we're missing things anymore. It's given our team a huge boost in morale," says Bailey.

Overall, the security team reports increased efficiency and effectiveness. "We now spend more valuable time proactively hunting through things in our environment because we know we have the Respond Analyst watching our backs," says Bailey.

Like many companies, Kyriba hopes to provide its security analysts with a pleasant and welcoming working environment in the hopes of retaining them for as long as possible. "We don't like the idea of having analysts look at a pane of glass for 10 to 12 hours a day, because that's what ultimately leads to the high turnover rate. Twelve hour shifts are brutal, and being alone in a quiet space at two in the morning is not a fun thing," explains Bailey.

Today, security analysts at Kyriba are able to spend the majority of time on threat hunting, incident response, and remediating vulnerabilities in the environment—all higher-value, more rewarding activities. They're able to achieve 24/7 coverage with human analysts working only from 7 a.m. to 7 p.m., and an on-call incident responder attending to the Respond Analyst's escalations overnight.

Adams and Bailey hope to retain their existing security team members for longer than ever before—an impressive feat in an industry known for high employee turnover rates. Because they're working smarter, and because they feel more successful, employees are far more satisfied. "One of the things in security operations and monitoring is that analysts want to be sure they're making a difference. Now they know they're doing work that matters," says Bailey.

Today Kyriba's nimble security team is having a big impact. WIth leaner human staffing levels, they're achieving world-class results, giving Kyriba global enterprise-grade security and the ability to meet stringent industry standards. This is achievable only through the use of intelligent automation. "With the Respond Analyst, life is easier because all the repetitive, mundane work has already been done for us. What we look at now are things we know we should be paying attention to," Bailey concludes.

To learn more about the Respond Analyst and how Robotic Decision Automation can make your security team more efficient and effective, request a demo today.

+1 833 737 7738

respond-software.com