CUSTOMER STORY

Financial Services Innovator Deploys Robotic Decision Automation for 24x7 security operations

Maintaining robust, enterprise-grade information security isn't easy for small to mid-sized organizations. Any company that processes high-value transactions and interacts directly with consumers makes an attractive target—especially if it doesn't have the resources to build and staff a large-scale security operations program.

Smaller or mid-sized financial services companies face the same security challenges as large banks and major investment firms. No matter its size, any company that processes or stores consumer financial data needs to ensure that information is well protected. This is especially important for organizations that process large volumes of high-value transactions. Our customer, the mortgage and title division of a Fortune 500 home building firm, needed to protect the data of its thousands of customers with a security team of only four full-time employees.

"We put a lot of time, resources, and effort into monitoring to make sure that we are protecting our networks and keeping our customers' data safe," explains the organization's CISO, an industry veteran and a security and risk management program leader, a conference organizer, and a security consultant. "In the mortgage and title industry, profits are transaction-based. There's only so much money we can make on each transaction." he says.

To achieve this goal, the team deployed the Respond Analyst side-by-side with their traditional SIEM solution. Comparing the results over the course of a year in which both solutions ingested the same data, they are highly confident that the intelligence and reliability of Robotic Decision Automation has made it possible for them to build a more efficient and cost-effective security program with no loss of detection accuracy.

Prior to implementing the Respond Analyst, the company had deployed a traditional Security Information and Event Management (SIEM) platform to aggregate and correlate log data from security sensors across their environment. They needed this log management solution to meet regulatory compliance requirements.

Industry: Financial Services

THE TECH ENVIRONMENT

Coverage Data: Multiple building sites nationwide; home sale revenues of $8 to $10 billion per year; security team of 4 full-time employees

Description of Security Environment: NIDS Sensors; SIEM solution

Existing Tools: Snort NIDS; SIEM from major vendor

Number of Security Incidents Escalated Prior to Implementation: over 10,000 per year

Number of Security Incidents Escalated Now: approximately 160 per year

> *If companies don't use security automation, they'll find that it's impossible to keep up. Automation is the only approach I've seen that can lead to truly effective monitoring of the gigantic number of security events that we all receive.*
>
> **Chief Information Security Officer**

respond

One year comparison:	SIEM	Respond Analyst
Hours tuning, managing, & writing rules	100s	0
Escalations for response	10,000s	160*

** 3 of the 160 escalations were missed by their SIEM*

> *We had a couple of cases where we were able to stop potential data loss because of the Respond Analyst, and also a couple of incidents of what appeared to be malicious software activity that we got in front of. If history is an example, the cost of the breaches that the Respond Analyst prevented could have been in the hundreds of thousands of dollars.*
>
> **Chief Information Security Officer**

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.

833.737.7738
respond-software.com

Their SIEM also provided a layer of defense by alerting when anomalies appeared in the log data it was collecting. It identified these anomalies according to a complex rule set containing pre-built rules and others the security team created.

"We were collecting a very large amount of log data," explains the CISO. "And we found that our SIEM required constant hours tuning, managing, & writing rules. We were getting alerts from our SIEM and it was easy to see that it was escalating a lot of false positives (alerts that were not malicious). Because of this, we'd dedicate hours of time and resources to update the rules in the SIEM to tune these alerts out." **On average, the security team was dedicating one quarter of their total working hours to this alert monitoring and tuning process.**

The organization decided to deploy the Respond Analyst in order to increase coverage and visibility within its environment. In particular, the team wanted to increase their security posture by introducing east-west traffic monitoring to detect attempts at lateral movement across the network, or threats that client-to-server monitoring might have missed. The team knew the installation of these additional detection devices would increase the number of alerts, but with the Respond Analyst they could handle the expansion capacity cost-effectively.

"Respond has been responsive to our feedback, and in turn the Respond Analyst performs better in our environment and provides the scale, speed, transparency and visibility we need to improve our security program."

Build a more secure future with the Respond Analyst

The benefits that this financial services company has seen since deploying the Respond Analyst include time savings, cost savings, and overall continuous improvement of their security program. Their security team is spending less time tuning the SIEM, and when they do tune it, are excluding more alerts, knowing that the Respond Analyst will catch anything that the SIEM misses. "The Respond Analyst has essentially added an additional analyst to our team," the CISO explains. "And that analyst's not working downstream from the SIEM—but instead is reviewing the full set of raw log data, and not being limited by what the SIEM rules deem worthy of escalation." Working together with the Respond Analyst, their human security team members are spending more time on higher-value tasks, including threat hunting and investigating potential vulnerabilities in the environment. "We're definitely more proactive now," he adds. "I think we have better defenses because of the higher quality of security monitoring."

To continue to provide industry-leading data protection to their customers, this financial services firm will work hand-in-hand with Respond Software to help develop additional capabilities within the Respond Analyst. They'll also work diligently to improve the maturity of their own security program, knowing that automation is the key to the future of security operations. "Things are only happening faster," says the CISO. **"If companies don't use security automation, they'll find that it's impossible to keep up. Automation is the only approach I've seen that can lead to truly effective monitoring of the gigantic number of security events that we all receive,"** he concludes.

respond

AFTER THE RESPOND ANALYST

160 incidents escalated out of

272M events monitored with

100% accuracy

* OVER 1 YEAR PERIOD

We Added a 20% Increase in Security Team Capability

- **24/7** EXTENDED COVERAGE
- **100s** OF HOURS SAVED TUNING SIEM
- **95%** ALERT NOISE REDUCTION
- **$100,000s** SAVED IN BREACH COSTS

Don't believe us? Get a demo today

respond