# Top 10 Bank Selected Devo SOAR to Free Up 93 Analyst Hours Per Week

CUSTOMER SUCCESS STORY

One of the oldest and largest investment banks in the United States is headquartered in New York and serves 100 markets in over 30 countries. The bank has over $1.5 trillion in assets under management and offers its clients expertise for each stage of the investment lifecycle.

This institution boasts a reputation for being one of the safest investment banks in the world; with so much at stake, security is paramount.

## ALERT FATIGUE

The bank's SOC works with over 400 hard-coded rules in the Splunk platform. These rules trigger alerts frequently, usually as false alarms, creating significant ongoing triage work for the SOC's security analysts.

One such rule,to detect traffic to bad URLs, is triggered from data collected from web proxy logs.

On average, this rule fires about 225 times a week, or over 900 times a month. Each time the alert lands in a security analyst's inbox, it requires an average 30 minutes of the analyst's time to triage. In total, the bank's SOC team spends over 127 analyst hours per week just keeping up with this one rule.

Out of the roughly 900 rule firings each month, only three typically required further escalation, with the other 897 determined to be false positives.

## MANUAL ALERT TRIAGE

When the bank's security analysts analyze an alert, they're able to distinguish a true threat from a false positive with a fair amount of accuracy. They manually check each alert against other suspicious activities such as unusual increases in files being transferred, spikes in network traffic, and attempts to reach other known bad URLs. They also cross-check with threat analysis sites such as VirusTotal.

In most cases none of these other suspicious activities are present, and the analyst is able to dismiss the alert confidently as a false positive. Thirty minutes later, the analyst annotates the alert as a false positive and marks it as reviewed.

## INTELLIGENT AUTOMATION

Seeking a better approach that employed Intelligent Security Automation, the bank set up Devo SOAR and created an automation workflow to mimic all the steps an analyst performed upon receiving one of these alerts.

The Devo SOAR platform was able to replicate all of the cross-checking and correlation the analyst previously had to do manually. It quickly identified the alerts that were false positives, and even annotated its analysis with an explanation, marking the alert as reviewed in the SIEM system, just as an analyst would.

Now when an analyst sees these alerts, they also see the Devo SOAR platform's recommended decision for responding to the alert, as well as the reasoning for making this decision.

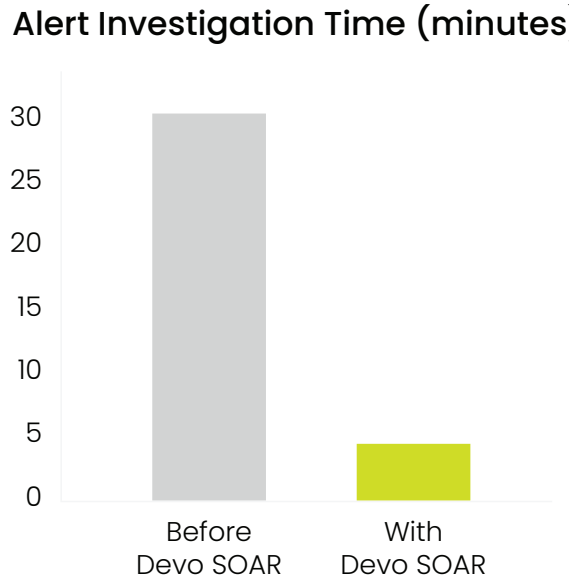
## THE RESULTS

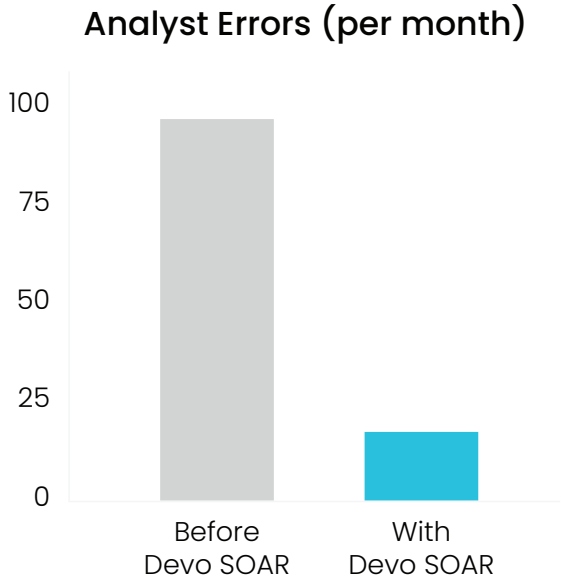
Using Devo SOAR for automation, the analysts were able to reduce the time they spent on each alert from 30 minutes to just 5 minutes. That is over a 80% reduction in time spent dealing with just this one SIEM rule.

Here's the math: 225 alerts/week x 25 minutes saved per alert = 93 analyst hours saved per week.

This reduced workload freed the bank's security analysts to spend more time on proactive threat hunting. Equally important, it also enabled analysts to focus on automating decisions for even more SIEM rules, promising ever-increasing time savings through security automation with Devo SOAR.

Not only did the SOC save time, the level of accuracy improved. In the course of manual investigations, security analysts made 98 mistakes (a 14% error rate), mischaracterizing threats or their severity levels. Once the SOC adopted Devo SOAR, error rates dropped from 98 per month to just 21 per month (a 3% error rate).



Having gained confidence in the Devo SOAR system and capitalizing on the time savings from this one use case, the SOC team then automated four additional use cases in a matter of weeks.

With the five use cases automated, they have realized a total of 308 hours per week in time savings.

## CONCLUSION

Before adopting Devo SOAR, the bank's SOC had been fundamentally lacking any automation of threat hunting and triage. Leveraging Devo SOAR's Intelligent Security Automation platform, the bank is able to:

1. Automate investigation processes easily and quickly
2. Save over 16,000 analyst hours annually (>7 FTE)
3. Achieve higher accuracy, reducing error rates by 3x
4. Reduce false positives by more than 95%
5. Free up analysts to focus on increased automation and proactive threat hunting

**Interested in learning more about Devo SOAR?**

**Read more on Devo.com or sign up for our trial to see the benefits first hand.**

**Devo**
255 Main Street
Suite 702
Cambridge, MA 02142



Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.