LogicHub™ Case Study

TOP 10 BANK

LogicHub

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.

With so much at stake, security is paramount. Fortunately, this institution boasts a reputation for being one of the safest investment banks in the world.

Alert Fatigue

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

One such rule is in place to detect traffic to bad URLs, and 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 a month, only three typically required further escalation, the other 897 are 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 like 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

The bank set up LogicHub's Intelligent Security Automation platform and created an automation workflow to mimic all the steps an analyst performed upon receiving one of these alerts.

The LogicHub 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 LogicHub platform's recommended decision for responding for the alert as well as the platform's reasoning for making this decision.

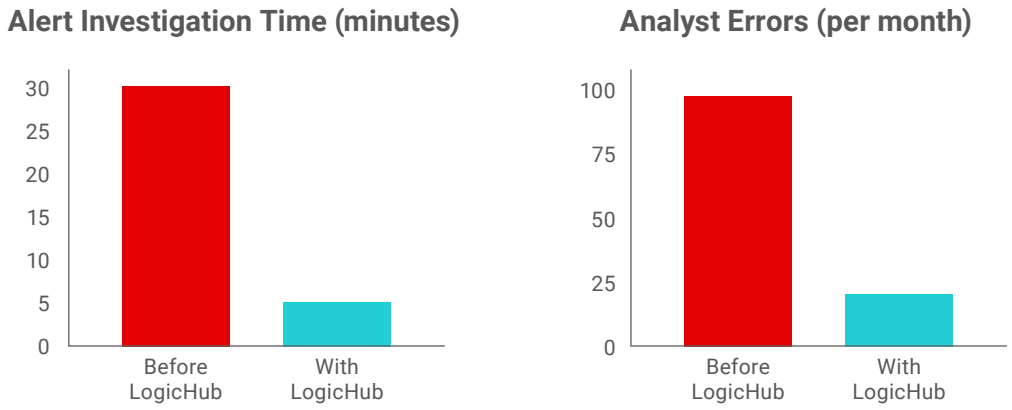
The Results

Using LogicHub's 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 working 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 an ever-increasing times savings from security automation.

Not only did the SOC save time, but it's accuracy improved. In the course of its manual investigations, security analysts made 98 mistakes (a 14% error rate), mischaracterizing threats or their severities. Once the SOC adopted LogicHub, error rates dropped from 98/month to 21/month (a 3% error rate).



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

Conclusion

Before adopting LogicHub, the bank's SOC had been fundamentally lacking any automation of threat hunting and triage. Leveraging LogicHub's Security Intelligence 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	**Achieved 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**

About LogicHub™

LogicHub is the leading Intelligent Security Automation platform. Its powerful decision engine coupled with highly flexible orchestration automation helps SOC teams deliver 10X the productivity gains, as compared to first-gen Security Orchestration Automation and Response (SOAR) solutions.

For more information, contact us at **logichub.com**