LogicHub

Case Study

# LogicHub Keeps Cyberthreats from Flying Under the Radar at One of the World's Largest Airlines

## Introduction

This company is among the 20 largest airlines globally. In 2019, it was operating more than 1,600 scheduled flights daily and offering vacation packages to over 90 destinations. With their extensive global footprint and large customer base, flight safety and security are top operational priorities. This includes maintaining a clean cybersecurity posture across the company's IT infrastructure. It's critical to ensure that malicious actors or system vulnerabilities aren't posing a threat to systems that keep the airline running safely and efficiently.

## The Challenge

The company already had a robust stack of security tools which included a SIEM, threat intelligence feeds, attack surface management, compromised credential detection, vulnerability checks, threat hunting, and more. Event logs and data feeds come from numerous sources across the organization and are consolidated in the SIEM. However, alerts from the SIEM were lacking in relevant event context, and getting retrieving it was a slow and time-consuming manual process.

The airlines security operations team was supplemented with a managed security service provider (MSSP) to manage and monitor components of their security infrastructure. When it detected or suspected threats, the MSSP forwarded alerts to the airline's security team. But there were too many alerts, and often they were false positives. There was no analysis or event context on the alerts to know which ones were critical to pursue and which could be ignored.

In short, the security team was suffering alert fatigue from the sheer volume of non-prioritized threat events that were surfacing and requiring attention. The company felt that the MSSP offering wasn't designed to address these problems and wanted to replace it, but the budget was tight. Nevertheless, the security analysts were buckling under the weight of the alerts and had to do something different to avoid the fate of a serious attack.

**Company Background:**

- Among the 20 largest airlines globally
- The company's roots date back nearly 85 years

**The Cybersecurity Challenges**

- MSSP was expensive and provided limited value
- SIEM alerts lacked context that was time consuming to gather
- Too many false positive alerts
- Small in-house security team

# The Solution

### LogicHub Earns Its Wings in a PoC

The company initially was attracted to LogicHub's SOAR+ platform because of strong relationships and technical integrations with Anomali, their threat intelligence platform, and QRadar, their SIEM. Both products are key components of the company's security stack, and a Proof of Concept (PoC) of the SOAR+ platform was initiated to test its ability to automate incident response workflows for the alerts coming from them, as well as other security tools.

From the start, the strong integrations with the existing security tools helped them get the SOAR+ platform in place and fully operating quickly. Then the security team was able to quickly build their first use case of the automation. They saw immediate value, and particularly liked the automated decision engine that allows them to replicate the expertise of a human analyst for L1/L2 investigations at higher speeds and with greater accuracy and consistency than when the work is done manually.

The company set stringent goals for the evaluation and LogicHub met or exceeded all of them. Having passed the tests of the PoC, the airline moved onto full implementation with numerous use cases. The company now uses LogicHub's SOAR+ to assist with vulnerability checks, threat hunting, reconnaissance validation, detection and response for malicious website traffic and credential-based attacks, reviews of threat bulletins, and more. They have gone beyond traditional SOAR use cases to attain better security outcomes.

### LogicHub SOAR+ Executes Many Use Cases

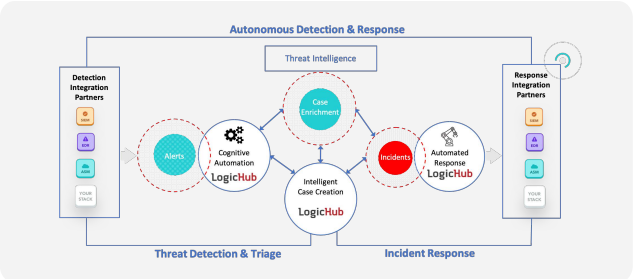
One of the first use cases put in place involves continuous security checks based on regular threat bulletins coming from Anomali. The airline's SOC analysts receive regular threat bulletins with potentially new threats that may exist in their environment. However, it takes too long to read the bulletins to identify new threats and then investigate each one to determine if it is a true threat or nothing of concern.

Now, LogicHub automatically parses relevant threat data out of the bulletins, GREPS the CVEs, submits them to an attack surface profiling platform (Randori), and then identifies and reports on all systems that are vulnerable to each CVE. LogicHub automation makes use of the existing security tools with structured workflows – i.e., playbooks that can be run without human intervention.

The SOC team is now able to automatically keep up with the latest threats and they no longer have to read the bulletins, which frees up their time for higher value work. At the same time, LogicHub provides automated escalation of real problems so they can be addressed much sooner.

Another use case involves mitigating attacks on a customer portal. This public-facing application is threatened often, and there are too many components of a web-based attack to quickly look up all relevant information to bring context to an incident in a timely manner. LogicHub automates the process of looking up relevant details such as the number of the account that's involved, which user agent is involved, how many compromised IP addresses, how many were using old passwords, and how many logins were successful. LogicHub quickly assembles the information so the security agent doesn't waste time doing this.

Now, the time to mitigation is greatly reduced, and the analysts are relieved of the menial data collection tasks that bog them down so they can apply their skills to higher level tasks.



## Tangible Benefits and Quantifiable ROI

Since the airline applied LogicHub's security orchestration, automation and response capabilities to these and many other use cases, the security team saw extensive value within just six months. They had the first use case running in under two weeks, which immediately reduced false positive alerts by 75%, simultaneously raising the level of accuracy and significantly lowering the mean time to resolution (MTTR).

They have had quantifiable ROI. LogicHub's automated playbooks have delivered easily quantifiable ROI, including replacing the need for at least 1 FTE (where their SIEM was unable to do so), and is now considered mission-critical to the security team. Playbooks analyze and triage all L1/L2 alerts and save at least 40 hours per week. And, they have completely replaced the need for their MSSP, delivering additional savings.

The company now has rapid incident response. Security analysts can execute certain actions with one click that previously would have taken a week or more to perform the number of steps involved—if they were at all possible.

LogicHub SOAR+ contributes to better security outcomes overall. Automating the process of moving from alerts to action has made the security team more resilient and adaptable. They now have the time to focus on strategic planning and more important security work. LogicHub delivers the visibility to find threats that they weren't seeing before.

What's more, there is cross-department value to using this platform. LogicHub allows the security team to automatically send threat reports and context to other groups. For example, they automatically send relevant fraud event context to the Fraud Department, and they help the Cyber Defense Team (i.e., the tools team) with process escalation.

With so many use cases and benefits of using the LogicHub SOAR+ platform, the airline's security team no longer fears that they have cyberthreats flying under their radar.


### The Solution

- LogicHub's SOAR+ platform
- Out-of-the-box integrations with existing security tools

### The Results

- Quantifiable ROI with at least 40 hours per week in time savings
- 75% of alert triage and security investigations are now automated
- Rapid "one click" incident response for many alerts
- Security team is now elevated to higher value work
- Small in-house security team