LogicHub

# Case Study: Health Services Provider

## Introduction

The Customer is a health services provider focused on rebuilding the health care delivery system through automation, with their platform removing the administration and third party burden on health providers. As a small company in a highly regulated industry vertical, they need the assurance of a dedicated team of security experts delivering 24/7 threat detection and incident response, but the overhead required to do so on their own is prohibitively expensive.

## The Challenge

Healthcare organizations face some of the largest cybersecurity challenges of any industry vertical. The value of healthcare data is higher for attackers than just about any other personal data, making it a prime target for cyber criminals. And the costs associated with a breach are higher than for any other industry, with the cost per record double that of financial institutions. Many of the reasons that make healthcare data so valuable are also why it is one of the most heavily regulated industries when it comes to protecting client data. That includes not just providers, but any organization that could potentially be targeted as an access point to locate and steal sensitive data like PHI.

Small organizations like the customer have the same business critical requirements to protect sensitive data, but typically have a fraction of the available resources to do so. Yet in the event of a breach, they face a significantly higher risk, with the cost per employee approaching nearly 20 times higher than for large organizations. Despite the critical need for deep threat detection and rapid incident response, the customer had only one FTE dedicated to security due to company size and resource constraints.

### Company Profile

- Healthcare services solutions provider
- Support over 1,000 clinics and other enterprises
- Fewer than 100 employees
- Heterogeneous environment with extensive cloud storage and infrastructure
- One Dedicated IT Security Professional

### Customer Needs

- 24/7 security, including monitoring, threat detection and incident response
- Access to an experienced incident investigation team
- Deeper visibility into
  - Cloud storage and infrastructure
  - Account Fraud and credential stuffing
  - Insider threats and employee misuse

## The Solution

The LogicHub MDR team has taken on the customer's issues and delivers an automation-driven approach to protect the integrity and confidentiality of their cloud storage, access control for authorized users, and monitoring their cloud based infrastructure. The main coverage areas include cloud-based infrastructure, cloud-based employee storage, user-based threats, account and credential fraud.

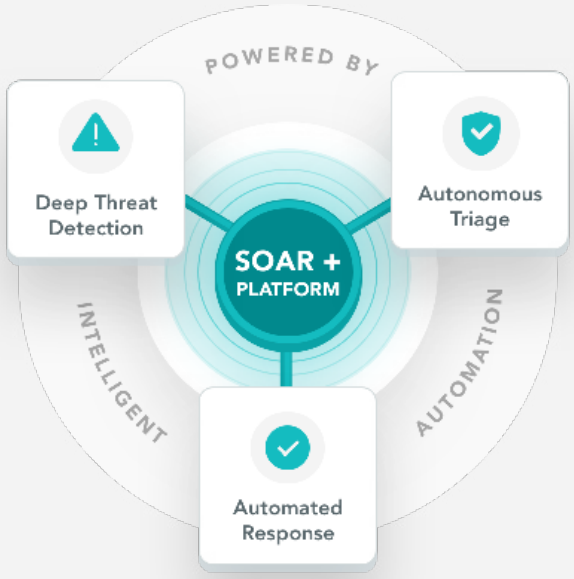
Among other things the customer benefits from algorithmic based brute force and password list attack detections. LogicHub's MDR team delivers 24x7 peace of mind, acting as a fully integrated part of their team. Currently the MDR team is running 24/7 automated detection covering 4 broad use cases, currently providing 40 specific deep threat detections across the areas of concern.

- 23 Detections for Cloud Infrastructure
- 4 Detections for Account Fraud
- 7 Detections for User Threats
- 6 Detections for Cloud Storage

## Value Delivered

The Customer's engagement with LogicHub empowers and extends the capacity of their small security force. Logichub's MDR team is able to detect and respond to threats around the clock without adding additional operating overhead. The partnership between the two delivers:

- Nearly 90% reduction in time spent investigating false positives
- Herd immunity from threat detections designed by Logichub long before they target organizations of a similar size and demographic
- Expert incident handling for new and unexpected issues and threats
- 24x7 detection and response coverage at a fraction of the cost of doing it on their own



LogicHub

# Detecting Account Fraud

## Problem Being Solved

Offerings for payment and collecting service payments means allowing customers to input payment data and pass it onto merchant services. Attackers will try to gain access to individual accounts for a multitude of reasons, many involve abusing the different merchant servicing APIs.

## Solution Workflow Summary

LogicHub playbooks can automatically baseline user authentication and API activity, profiling a broad range of data points, including the typical time it takes to enter the payment information, number of errors encountered, and the performance monitoring of access and api utilization. Using this data, LogicHub has created playbooks dedicated to hunting within the realtime and baselined data for signs of abuse.

## Playbook Benefit

- Continuously monitors global authentication, api utilization and service responses.
- Rapidly detects, investigates and escalates any suspicious or malicious activity to prevent unauthorized access from resulting in potentially damaging data exfiltration or malicious behavior
- Time-based and time-aware detections reduce false positives, allowing real threats to be addressed faster

## Integrations used

The playbook integrates with the following (category of) tools to automatically (one-click or fully automated) perform various actions like blocking of IOCs and the creation of support tickets.

- Web Access/Error Logs
- APM Logs
- Whois
- Threat Intelligence sources

LogicHub

# Protecting Cloud Infrastructure

## Problem Being Solved

The advent and increasing adoption of cloud-based infrastructure has led to a shared model of security where misconfigurations have led to many costly breaches. With the dynamic nature of cloud infrastructures, real time monitoring of changes is necessary to highlight issues more quickly.

## Solution Workflow Summary

LogicHub playbooks can automatically query and correlate cloud infrastructure and audit logs. Changes that occur without apparent authorization or that expose data are created via new or unknown automations are identified and escalated to the app opriate teams for confi mation and acceptance or remediation.

## Playbook Benefit

- Continuously monitor API access, IAM calls and scripted automations
- Rapidly detect, investigate and escalate any suspicious or malicious activity and directly call out changes or other activity done without prior authorization being ticketed

## Integrations used

The playbook integrates with the following (category of) tools to perform detections on raw data to enhance and correlate the data into a decision point.

- Cloud Audit Logs
- Cloud Administration Logs
- Change Management/IT Ticketing System
- User Lists

LogicHub

# Detecting Compromised Credentials/Insider Threats

## Problem Being Solved

User monitoring is necessary  because stolen credentials are a significant threat that is particularly difficult to detect because they emulate valid user activity--and any user's credentials can be compromised. Insider threats are another critical reason for monitoring and analyzing user behavior. But monitoring user behavior for suspicious and/or malicious activity is often too manual and time consuming, and requires the analysis and correlation of large amounts of data from numerous sources.

## Solution Workflow Summary

LogicHub playbooks can automatically baseline user activity from authentication to daily tasks and functions. These data points for a baseline that the Logichub playbooks may hunt through and correlate with for potential abuse or threats. Using data generated in real time from user activities, comparing against physical and logical IOC's as well as historical user data allows Logichub to escalate possible threats for review, and to call out known or proven malicious chains that affect user behaviors.

## Playbook Benefit

- Continuously monitor user data and calculate baselines for user behavior.
- Rapidly detect, investigate and escalate any suspicious or malicious activity correlating indicators from user behavior, system activity, and threat or physical intelligence.
- Time-based and time-aware detections reduce false positives.

## Integrations used

The playbook integrates with the following (category of) tools for data, correlation and context enhancement.

- Authentication logs
- VPN logs
- Whois
- Threat Intelligence sources
- Process creation logs

LogicHub

# Cloud Storage

## Problem Being Solved

Providing offerings for paying and collecting service payments requires allowing customers to input payment data and pass it onto merchant services. Attackers will try to gain access to individual accounts for a multitude of reasons, many involve abusing the different merchant servicing API's

## Solution Workflow Summary

LogicHub playbooks can automatically baseline user authentication and API activity, profiling a broad range of data points, including the typical time it takes to enter the payment information, number of errors encountered, and the performance monitoring of access and API utilization. Logichub analyzes this data with automated playbooks dedicated to hunting within the realtime and baselined data for signs of abuse.

## Playbook Benefit

- Continuously monitor global authentication, API utilization and service responses.
- Rapidly detect, investigate and escalate any suspicious or malicious activity rapidly to prevent unauthorized access from resulting in potentially damaging data exfiltration or malicious behavior
- Time-based and time-aware detections reduce false positives.

## Integrations used

The playbook integrates with the following (category of) tools to perform various actions like blocking of IOCs and the creation of support tickets on ITSM.

- Cloud Storage user activity logs
- Audit and Admin Logs
- Whois
- Threat Intelligence sources
- Geo-location services