LogicHub

Customer Case Study

SOAR+ for Compliance Automation

A leading Fintech provider's security operations team is challenged to secure critical confidential client data while also meeting numerous compliance requirements. Many of the compliance-related activities involve slow, manual processes that take time away from critical security activities or are too time consuming to perform as needed.

In order to overcome these issues, they implemented LogicHub's SOAR+ platform to automate numerous compliance and security tasks, allowing them to address more use cases, respond faster, and increase operating capacity. LogicHub has worked with the client to help build and implement multiple playbooks that help eliminate false positives, automate time consuming and repetitive manual tasks, and meet critical compliance requirements.

Primary Use Cases

- Automate time consuming and manual compliance related account verification
  - Privileged user account certification
  - Inactive account management
- High volume, automated alert triage and response for SIEM and phishing alerts
- Automate manual administrative tasks like account off-boarding

About the Customer

Leading provider of personalized finance platforms for global money management.

Industry:	Fintech
No. of Employees:	1,400
Revenue:	$1 billion+
Security Team Size:	15 Analysts

Integrated Platforms

AbuseIPDB	*Powershell*
Active Directory	*VirusTotal*
Amazon AWS	*Palo Alto WildFire*
Case Management	*Amazon EC2*
Exchange (EWS)	*File Tools*
Falcon Host Sandbox	*ServiceNow*
MongoDB	*Splunk*
PassiveTotal	*SSH*

Access Recertification for Privileged Users

Customer Use Case:

Compliance requires that all privileged user accounts are verified for legitimacy every quarter. The original process required manual account lookups for hundreds of users, with individual managerial verification, to either reauthorize or revoke based on the response.

LogicHub Automated Solution

- Retrieves all relevant user detail and emails a verification form to their manager
- Based on each manager's response, either access is verified or case is created to revoke privileges for the account
- Users lacking an assigned manager are flagged for data cleanup

Benefits

- Immediately identified over 800 users requiring recertification
- Automated a previously manual process from hours to minutes
- Freed skill personnel to focus on skilled security activities

Inactive Account Validation

Customer Use Case:

Compliance requires any account that has been inactive for longer than 90 days to be verified and either reset or revoked. This was such a time consuming manual effort that the customer lacked the resources to carry out the require process and it was not being done.

LogicHub Automated Solution

- Checks daily for any account inactive for longer than 90 days, excluding any account on a known inactive list
- Notifies users (with 4 additional reminders) that they have 12 days to login or the account will be deleted
- Depending on user response, accounts are either reset or deleted

Benefits

- Identified and removed over 300 inactive accounts in the first pass
- Automate continuous compliance for previously infeasible process
- Built auditable system of record for regulatory/audit compliance

LogicHub

301 N Whisman Rd Mountain View, CA 94043
info@logichub.com • tel 650- 262-3756
logichub.com