Leading Fintech Selects Devo SOAR for Compliance Automation

CUSTOMER SUCCESS STORY

SUMMARY

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 effectively as needed.

In order to overcome these issues, the SOC team implemented Devo SOAR to automate numerous compliance and security tasks, allowing them to address more use cases, respond faster, and increase operating capacity. Devo 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

INDUSTRY: Finance

COMPANY PROFILE

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

USE CASE: ACCESS RECERTIFICATION FOR PRIVILEGED USERS

Description

- 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 lookups.

Devo SOAR automated solution

- Retrieves all relevant user detail and emails a verification form to their manager
- Based on each manager's response, 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 additional critical security activities

USE CASE: INACTIVE ACCOUNT VALIDATION

Description

- 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 required process, and it was not being properly conducted.

Devo SOAR 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
- Automated continuous compliance for previously infeasible process
- Built auditable system of record for ensuring regulatory/audit compliance

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**.