A health services provider, focused on reducing administration and third-party burdens on health providers, decided to rebuild their health care delivery platform through automation. As a small company in a highly regulated industry vertical, they needed the assurance of a dedicated team of security experts delivering 24/7 threat detectietiit 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

THE SOLUTION

The Devo SOAR team delivers an automation-driven approach to protect the integrity and confidentiality of the client's cloud storage, access control for authorized users, and monitor 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. Devo's SOAR team delivers 24x7 peace of mind, acting as a fully integrated part of the client's team. Currently the Devo team is running 24/7 automated detection covering 4 broad use cases, 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

RESULTS

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

- Nearly 90% reduction in time spent investigating false positives
- Herd immunity from threats, via detections designed by Devo SOAR, 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

tn3.1 (t)9.4 (d(•)1(B.6 1 (t)9.4 (d(•)1((i)4.1 (t)-22 (y)t)1.4 (i)-6b

Integrations Used

- The Devo SOAR playbook integrates with the following (category of) tools to automatically (one-click or fully automated) perform various actions like blocking of Incidents of Compromise (IOCs) and the creation of support tickets:
  - Web Access/Error Logs
  - APM Logs
  - Whois
  - Threat Intelligence sources

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 quickly highlight issues.

Solution Workflow Summary

- Devo SOAR playbooks can automatically query and correlate cloud infrastructure and audit logs. Changes that occur without apparent authorization,that expose data or are created via new or unknown automations are identified and escalated to the appropriate teams for confirmation 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

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 the attackers 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

- Devo SOAR playbooks can automatically baseline user activity from authentication to daily tasks and functions. These data points form a baseline that the Devo SOAR playbooks may hunt through and correlate with for potential abuse or threats. Using data generated in real time from user activities and comparing against physical and logical IOC's as well as historical user data allows Devo SOAR 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 of 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

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