Healthcare Service Provider selects Devo SOAR for around-the-clock coverage

CUSTOMER SUCCESS STORY

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 detection and incident response, since the cost 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 such as Protected Health Information (PHI).

Small organizations such as this customer have the same business critical requirements to protect sensitive data as larger healthcare organizations,, but typically have a fraction of the available resources to do so. Yet in the event of a breach, they face 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.

INDUSTRY: Health Services

COMPANY PROFILE

- Healthcare services solutions provider
- Supports 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 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 fraction of the cost of doing it on their own

DETECTING ACCOUNT FRAUD

Problem Being Solved

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

Solution Workflow Summary

- Devo SOAR 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, Devo SOAR creates playbooks dedicated to hunting for threats within the real-time and baselined data.

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 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
Cambridge, MA 02142