Major Airline Keeps Cyberthreats from Flying Under the Radar

Security Orchestration Automation and Response with Devo SOAR

CUSTOMER SUCCESS STORY

THE CHALLENGE

The small security operations team for a major national airline was stretched thin and suffering from alert fatigue trying to keep up with cyberthreats. While they had a robust security stack, and consolidated events in their SIEM, the alerts lacked important context, resulting in time-consuming manual follow-up.

The in-house team was supplemented with an MSSP, but the service provider bombarded them with too many alerts, far too many false positives, and didn't provide analysis or context on security events.

While the team needed help consolidating alerts more efficiently and automating incident response, they wanted to build on to their existing security stack.

THE SOLUTION

The initial use case was conducting continuous security checks based on threat bulletins from security vendor Anomali. Evaluating and acting on each threat, however, was a manual time-consuming and cumbersome process. Instead, using Devo SOAR relevant threat bulletins are automatically parsed, using GREP to look for relevant CVEs, and submitting results to Randori for attack profiling, thus automating incident response and case management.

Working in close collaboration with Devo SOAR experts, the security team developed custom playbooks to automate all steps without the need for human interaction.

Subsequent playbooks have been developed for a wide range of use cases including vulnerability checks, threat hunting, reconnaissance validation, detecting malicious website traffic, stopping credential-based attacks, and reviewing threat bulletins.

INDUSTRY: Airline

COMPANY PROFILE

- One of the top 20 largest airlines globally
- Multi award-winning airline
- 85 years of operation and a fleet of more than 400 aircraft
- Serving more than 220 destinations on six continents
- Carrying more than 50 million passengers a year

SECURITY SITUATION:

- Small in-house security team
- MSSPs too expensive, provided little value
- SIEM alerts lacked context
- Too much time spent on handling alerts and false positives

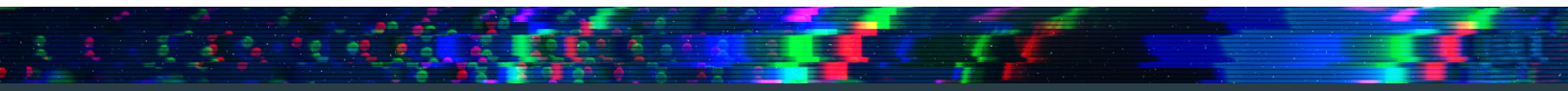
RESULTS

- Initial use case running in under two weeks, immediately reducing false positive rate by 75%
- Devo SOAR triages all L1/L2 alerts, saving over 40 hours per week (1 FTE)
- Dramatic improvement in accuracy and faster response time (MTTR)
- Replaced legacy MSSP, with significant cost savings
- Rapid incident response with one-click automation

WHY DEVO SOAR

- Out-of-the-box integration with Anomali, QRadar, Randori, and other key security tools
- Decision Automation captures analyst expertise while automating detection and response
- Dramatically better speed and accuracy than manual processes
- Close collaboration with Devo SOAR experts on creation of playbooks
- Rapid time-to-value across a wide range of use cases

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**.