Devo SOAR

A Milestone in the Journey to the Autonomous SOC

SOLUTION BRIEF

SIEM AND SOAR COMBINATION ACCELERATES JOURNEY TO THE AUTONOMOUS SOC

Security teams face a multitude of daily challenges, from the ever-increasing number and complexity of cyberthreats to too many disparate security tools with too many alerts and repetitive manual workflows, to too few qualified analysts. This prevents teams from responding to threats consistently and with the accuracy and speed required. The result: poor ROI from the investment in security tools.

A shift in how security teams solve these challenges is urgently needed. This change requires better technology, not futile attempts to source scarce and overworked security analysts to try and respond to a barrage of cyberthreats.

Cloud-native security technologies address many of the challenges by eliminating the ad-hoc, manual activities security teams wrestle with each day, but this leads to alert fatigue (in the 2021 Devo SOC Performance Report™, 61% of survey respondents cited "too many alerts to chase" as a key reason working in the SOC is painful) and results in teams spending an inordinate amount of time on tasks better handled by smart automation and intelligent autonomous solutions.

Devo SOAR Benefits:

Increased Productivity 10 to 20x
More alerts addressed without dependency on future headcount

Boost Efficiency 10 to 50x
Reduction in MTTR from hours to minutes

Achieve Consistency 5 to 10x
Less errors compared to human analysts and codified processes

WHAT DEVO SOAR PROVIDES TO DEVO CUSTOMERS

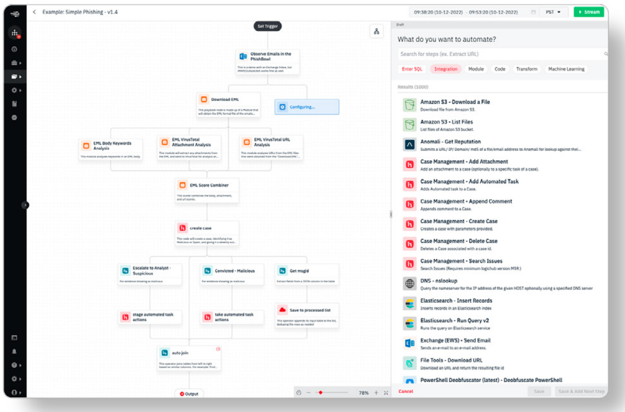
Devo SOAR is a SaaS cloud-native security orchestration, automation and response (SOAR) solution that improves SOC efficiency – as much as 10x – by enabling security teams to address the growing barrage of cyberattacks, as well as scaling and augmenting their existing security talent.

Devo SOAR provides intuitive case management that adapts to your workflow and enables security teams to track and collaborate seamlessly on security incidents. It also continuously captures the metrics that matter most to your team and stakeholders so you can ensure your organization completely understands your security outcomes. And with more than 300 integrations, Devo SOAR seamlessly integrates with security teams' environments. If you need a new integration, Devo SOAR will create it.

DEVO SOAR PLAYBOOK

With its no-code capabilities, Devo SOAR is significantly easier to implement and use than competing SOARs. That ensures fast time to value and yields a return on investment within just 30 days. Devo SOAR customers see upwards of a 10X improvement in MTTR, can address 10 to 20x more alerts with the same number of security analysts, and realize up to 95% fewer false positive alerts. Compared to other leading SOAR solutions, Devo SOAR's patented decision automation technology has proven to exceed human accuracy. This enables analysts to fully trust the decisions and actions it makes during playbook execution, which boosts SOC performance.

During setup, Devo SOAR AuDRA — an AI-driven technology that augments your team — provides guided playbook creation assistance. AuDRA, which sits side-by-side with analysts, enables no-code playbook creation each step of the way — no matter how advanced you need the playbook to be. This makes SOAR capabilities accessible to security teams of all experience levels.


Example: Simple Phishing - v1.4
09:38:20 (10-12-2022) - 09:53:20 (10-12-2022)
PST
Stream
Set Trigger
Observe Emails in the PhishBowl
Download EML
Configuring...
EML Body Keywords Analysis
EML VirusTotal Attachment Analysis
EML VirusTotal URL Analysis
EML Score Combiner
create case
Escalate to Analyst - Suspicious
Convicted - Malicious
Get msgid
stage automated task actions
take automated task actions
Save to processed list
auto join
Output
78%
Draft
What do you want to automate?
Search for steps (ex. Extract URL)
Enter SQL
Integration
Module
Code
Transform
Machine Learning
Results (1000)
Amazon S3 - Download a File
Download file from Amazon S3.
Amazon S3 - List Files
List files of Amazon S3 bucket.
Anomali - Get Reputation
Case Management - Add Attachment
Add an attachment to a case (optionally to a specific task of a case).
Case Management - Add Automated Task
Adds Automated task to a Case.
Case Management - Append Comment
Appends comment to a Case.
Case Management - Create Case
Creates a case with parameters provided.
Case Management - Delete Case
Deletes a Case associated with a case id.
Case Management - Search Issues
DNS - nslookup
Elasticsearch - Insert Records
Inserts records in an Elasticsearch index
Elasticsearch - Run Query v2
Runs the query on Elasticsearch service
Exchange (EWS) - Send Email
Sends an e-mail to an e-mail address.
File Tools - Download URL
PowerShell Deobfuscator (latest) - Deobfuscate PowerShell
Cancel
Save
Save & Add Next Step

THE MANY BENEFITS OF THE AUTONOMOUS SOC

Devo is charting the path forward so our customers can realize the autonomous SOC's many game-changing benefits. The autonomous SOC will reinvent how security teams work by providing complete visibility, analytics and access to the latest community expertise and content. The autonomous SOC leverages advanced capabilities such as automation, AI, and machine learning so teams can focus on critical issues to perform faster, more effective incident response and detection to resolve threats on large-scale, cloud and legacy infrastructures. The addition of SOAR capabilities to the Devo Platform further accelerates Devo's ability to deliver on this vision.

Devo is the only cloud-native platform that provides:

- The most scalable and performant enterprise log management for full visibility across the organization
- Threat detections and security content crafted by Devo SciSec, our security research and data science team, that deliver continuous value to security teams
- Autonomous hunting to shift the threat investigation starting point for analysts from alerts to end-to-end threat stories
- Autonomous alert triage, investigation, and response at machine speed, boosting the efficiency of analysts by 10x
- No-code capabilities across threat hunting, threat detection, and response along with patented capabilities to speed both time-to-deploy playbooks and enable highly accurate response actions to stop cyberattackers in their tracks
- Endless extensibility with comprehensive APIs and data connectors to ensure organizations can seamlessly integrate it with the best-of-breed technologies they use

Are you ready to learn more about Devo SOAR?
Contact your sales representative to schedule a demo or visit our website to learn more.

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

© 2022 Devo All Rights Reserved

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**.