Devo SOAR

Reduce Threat Detection, Investigation, and Response Workload by 80%

SOLUTION BRIEF

SECURITY TEAMS STRUGGLE TO ADDRESS THE GROWING BARRAGE OF CYBER ATTACKS

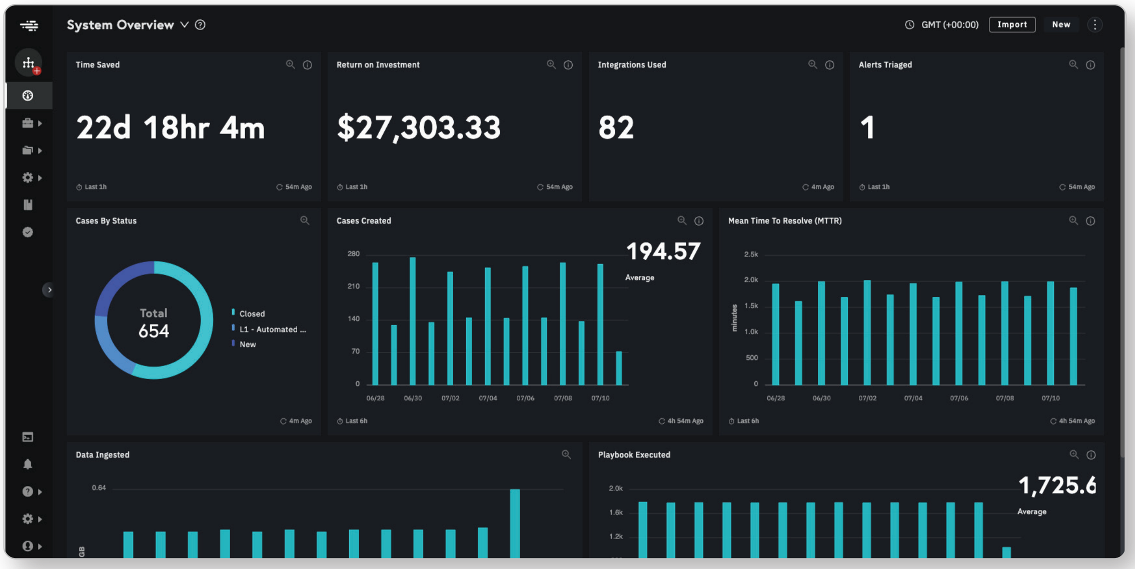
Today's SOCs face an ever-increasing number and complexity of cyber threats, exacerbated by too many disparate security tools generating a high volume of alerts. This barrage of alerts overwhelms a limited number of analysts burdened by repetitive, manual workflows. As a result, security teams cannot consistently respond to threats with the accuracy and speed they need to protect their organization.

SOCs need better technology to eliminate the ad-hoc, manual approach to detecting and responding to threats. By embracing security automation, analysts can spend more time hunting for adversaries and less time performing repetitive, low-value tasks.

DEVO SOAR PROACTIVELY REDUCES SOC WORKFLOW

Devo SOAR, a SaaS cloud-native security orchestration, automation, and response (SOAR) solution, uses AI-powered playbooks and decision automation to handle any volume of alerts consistently and accurately without scaling headcount while reducing response times from hours to minutes.

Devo SOAR is a key element of the Devo Security Data Platform. Powered by Devo's HyperStream data analytics engine and security content crafted by Devo's research and data science teams, Devo SOAR integrates seamlessly with all of the platform's SIEM capabilities, including Devo Behavior Analytics, Collective Defense, and DeepTrace, to remediate threats and respond to attacks.



Devo SOAR utilizes AI-powered playbooks and decision automation to handle any volume of alerts.

GO BEYOND TRADITIONAL SOAR SOLUTIONS AND UNLEASH AN EFFECTIVE AND EFFICIENT SOC

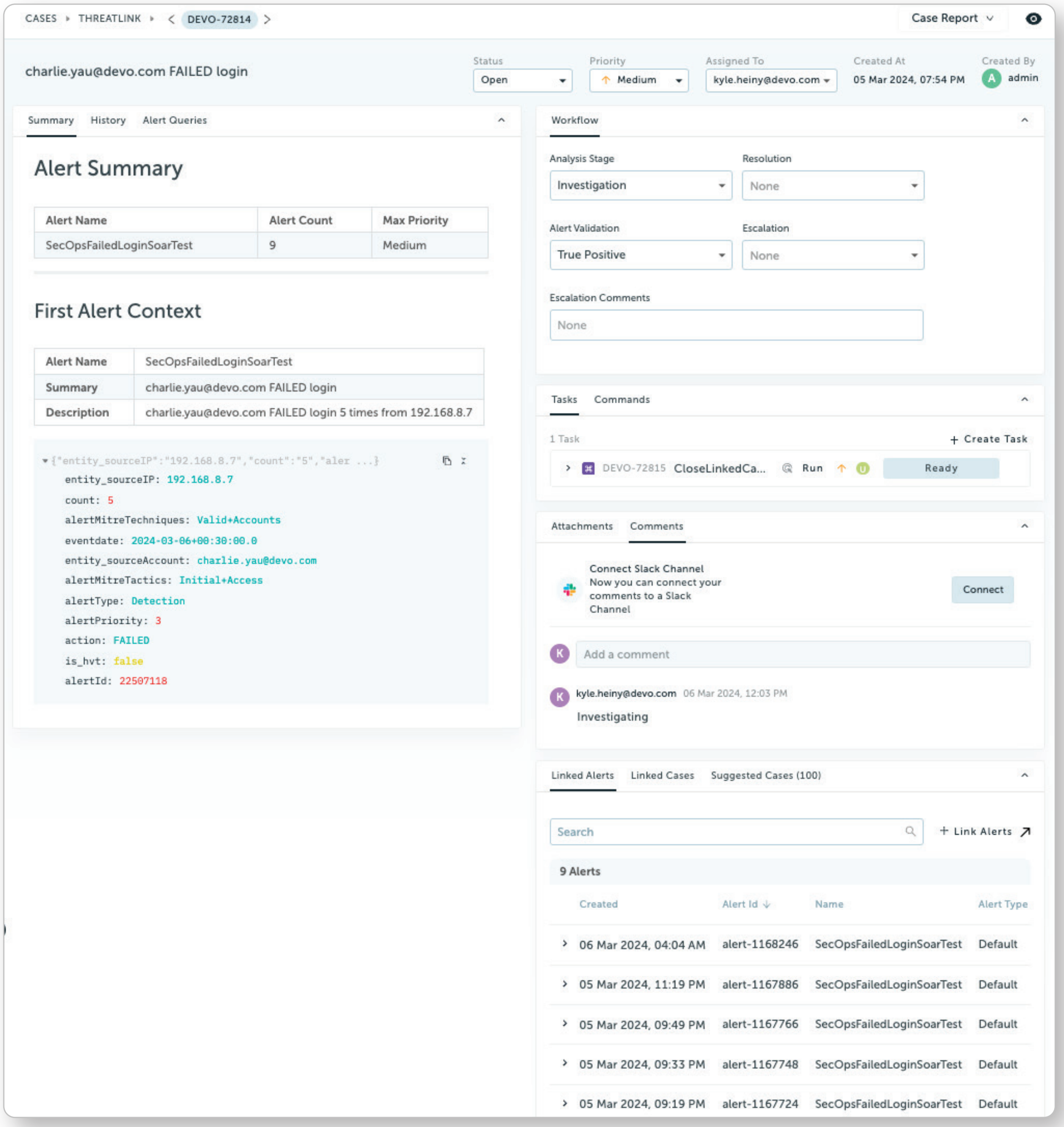
Devo SOAR helps SOC teams perform faster, more effective incident response and detection to resolve threats on large-scale, cloud, and legacy infrastructures:

Intuitive Case Management: Devo SOAR case management provides a systematic approach to tracking and collaborating on security investigations, ensuring consistency of standard operating procedures.

Focus Efforts on the Cases that Matter: Devo's ThreatLink playbook automatically correlates and enriches alerts into high-fidelity cases, reducing thousands of alerts to tens of cases per day.

Continuous Measurement and Reporting: Devo SOAR continuously captures the metrics that matter most to security teams and stakeholders so you can ensure your organization completely understands your security outcomes.

Seamless Integration: Devo SOAR ships with more than 300 integrations, easily integrating with security teams' environments.



charlie.yau@devo.com FAILED login

Status: Open
Priority: Medium
Assigned To: kyle.heiny@devo.com
Created At: 05 Mar 2024, 07:54 PM
Created By: admin

Alert Summary

Alert Name	Alert Count	Max Priority
SecOpsFailedLoginSoarTest	9	Medium

First Alert Context

Alert Name	SecOpsFailedLoginSoarTest
Summary	charlie.yau@devo.com FAILED login
Description	charlie.yau@devo.com FAILED login 5 times from 192.168.8.7

```
▾{"entity_sourceIP":"192.168.8.7","count":"5","aler ...}
    entity_sourceIP: 192.168.8.7
    count: 5
    alertMitreTechniques: Valid+Accounts
    eventdate: 2024-03-06+00:30:00.0
    entity_sourceAccount: charlie.yau@devo.com
    alertMitreTactics: Initial+Access
    alertType: Detection
    alertPriority: 3
    action: FAILED
    is_hvt: false
    alertId: 22507118
```

Analysis Stage: Investigation
Resolution: None
Alert Validation: True Positive
Escalation: None
Escalation Comments: None

1 Task
DEVO-72815 CloseLinkedCa... Run Ready

Connect Slack Channel
Now you can connect your comments to a Slack Channel

Add a comment

kyle.heiny@devo.com 06 Mar 2024, 12:03 PM
Investigating

Search

9 Alerts

Created	Alert Id ↓	Name	Alert Type
06 Mar 2024, 04:04 AM	alert-1168246	SecOpsFailedLoginSoarTest	Default
05 Mar 2024, 11:19 PM	alert-1167886	SecOpsFailedLoginSoarTest	Default
05 Mar 2024, 09:49 PM	alert-1167766	SecOpsFailedLoginSoarTest	Default
05 Mar 2024, 09:33 PM	alert-1167748	SecOpsFailedLoginSoarTest	Default
05 Mar 2024, 09:19 PM	alert-1167724	SecOpsFailedLoginSoarTest	Default

Devo SOAR case management with ThreatLink automatically reduces thousands of alerts to tens of cases per day.

ORCHESTRATE AND AUTOMATE THE MOST CRITICAL USE CASES

Devo SOAR addresses your most critical and time-consuming security operations workflows, improving completion time up to a factor of 10.

Use Case:

THREAT DETECTION AND TRIAGE

The Challenge: Organizations often need help rapidly detecting and responding to security threats due to the sheer volume of alerts and the complexity of analysis.

The Devo SOAR Solution: Devo SOAR leverages the Devo Security Data Platform to automate the collection and analysis of threat data from various sources, enabling faster threat detection and triage. Devo SOAR then orchestrates an appropriate response based on predefined standard operating procedures, using case management and ThreatLink to reduce their caseload by upwards of 80%.

Benefits: Implementing Devo SOAR reduces response time to emerging threats, minimizes the likelihood of human errors in the threat response process, and improves the efficiency and effectiveness of threat management operations. One customer reduced 25,000 alerts to 11 cases using Devo SOAR Case Management and ThreatLink.

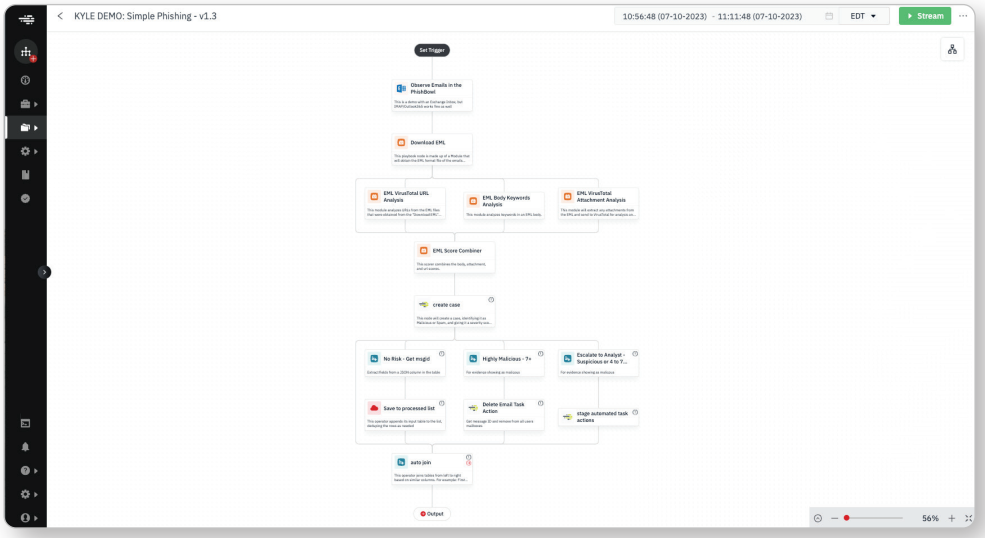
Use Case:

INCIDENT MANAGEMENT AND COLLABORATION

The Challenge: Managing cybersecurity incidents can be overwhelming due to the need for coordination between different teams and tools.

The Devo SOAR Solution: Devo SOAR, enabled by the Devo Security Data Platform's unmatched visibility at scale, facilitates centralized incident management, allowing security teams to collaborate effectively. It integrates various security tools and provides a unified platform for managing incidents.

Benefits: Devo SOAR significantly streamlines incident management by automating workflows and integrating security tools, leading to more efficient response protocols. With enhanced collaboration on a unified platform, built-in support for chat environments (Slack, etc.), and on-demand automated commands, security teams can pivot and quickly gather new information, resolving security incidents faster and more effectively. The result is improved operational efficiency and a minimized impact from security breaches, enhancing the organization's overall security posture.


KYLE DEMO: Simple Phishing - v1.3
10:56:48 (07-10-2023) - 11:11:48 (07-10-2023)
EDT
Stream
Set Trigger
Observe Emails in the PhishBowl
This is a demo with an Exchange Inbox, but IMAP/Outlook365 works fine as well
Download EML
This playbook node is made up of a Module that will obtain the EML format file of the emails...
EML VirusTotal URL Analysis
This module analyzes URLs from the EML files that were obtained from the "Download EML"...
EML Body Keywords Analysis
This module analyzes keywords in an EML body.
EML VirusTotal Attachment Analysis
This module will extract any attachments from the EML and send to VirusTotal for analysis an...
EML Score Combiner
This scorer combines the body, attachment, and url scores.
create case
This node will create a case, identifying it as Malicious or Spam, and giving it a severity sco...
No Risk - Get msgid
Extract fields from a JSON column in the table
Highly Malicious - 7+
For evidence showing as malicous
Escalate to Analyst - Suspicious or 4 to 7...
For evidence showing as malicous
Save to processed list
This operator appends its input table to the list, deduping the rows as needed
Delete Email Task Action
Get message ID and remove from all users mailboxes
stage automated task actions
auto join
This operator joins tables from left to right based on similar columns. For example: First...
Output
56%

Devo SOAR empowers security teams to easily create playbooks and implement use cases quickly.

Use Case:

IMPROVED SOC WORKFLOW

The Challenge: Taking the documentation of a standard operating procedure (SOP) and turning it into automation that can be used quickly without having to write Python code or build connectors manually.

The Devo SOAR Solution: Devo SOAR empowers security teams to easily create playbooks and implement use cases quickly and without having to write code. Devo's Audra – AI-driven technology – provides guided playbook creation codifying the knowledge of an expert security engineer.

Benefits: Devo SOAR strengthens an organization's security posture by accelerating security operations workflows such as threat investigation and vulnerability management, guiding security teams to build the right automations without coding while integrating with end systems to favorably impact security posture.

BENEFITS AND OUTCOMES

Devo SOAR provides a tremendous improvement in the productivity of your security operations team and increased consistency in executing security workflows. Security organizations will achieve:

Increased Productivity: Reduce alert triage workload up to 80%

Greater Efficiency: Accelerate investigations up to a factor of 10

Improved Process Consistency: Ensure standard operating procedures are executed across multiple incidents

Are you ready to learn more about Devo SOAR?

Contact your sales representative or visit Devo.com

Devo
3 Center Plaza
Suite 302
Boston, MA 02108

© 2024 Devo All Rights Reserved

Devo unleashes the power of the SOC. The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence global enterprises need to defend expanding attack surfaces. An ally in keeping your organization secure, Devo combines the power of people and AI to augment security teams, leading to better insights and faster outcomes.