Devo Flow

Detect, Investigate and Resolve Threats Faster with Streaming Analytics

SOLUTION BRIEF

INCREASE YOUR SOC EFFECTIVENESS AND REDUCE YOUR MTTD/MTTR WITH STREAMING ANALYTICS

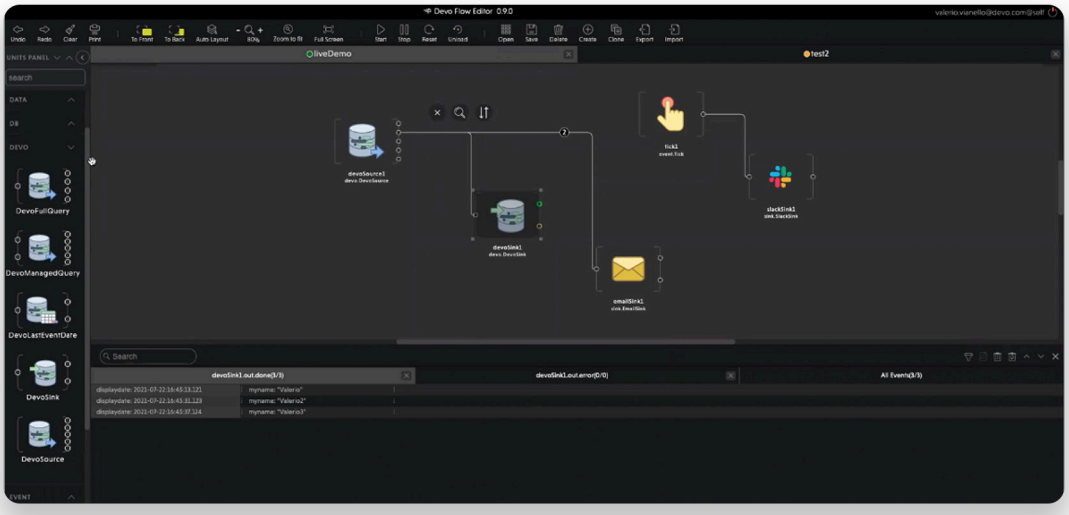
With a growing threat landscape and limited resources, you need security tools that extend the reach of your security team by helping them work faster and more effectively. The volume of data you need to sift through to detect malicious indicators keeps growing continuously, which is why you need the ability to run analytics in real time to take immediate action to stop threats promptly and decisively.

The Devo Platform is the cloud-native logging and security analytics solution that empowers you with the speed, scale and clarity to achieve full visibility. With Flow, Devo delivers powerful streaming analytics that enable you to stay ahead of cyberattackers.

Flow gives you the ability to process and analyze data in motion so you can accelerate threat detection and focus your valuable time on mitigating the threats that put your organization at risk. With granular, actionable insights in real time, you will be able to detect, investigate and resolve threats rapidly, reducing your organization's MTTD and MTTR.

FLOW BOOSTS THE CORRELATION, ALERTING AND ANALYTICS CAPABILITIES OF THE DEVO PLATFORM

Part of the Devo Platform, Flow is an easy-to-use visual editor that extends the correlation, alerting and analytics capabilities of Devo. It gives you the flexibility to deploy predefined or customized use cases and leverage powerful automation for deeper analysis to gain a defensive advantage against threat actors.



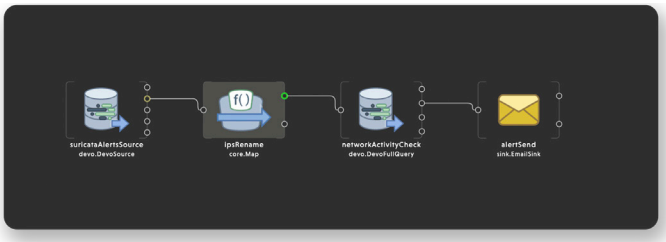
With Flow, you will be able to build complex alerts for more accurate detections, architect workflows for valuable correlations, as well as enrich, transform and combine your data stored in the Devo Platform with third-party sources — all through an easy-to-use UI.

FLOW UNLOCKS VALUABLE USE CASES TO STRENGTHEN YOUR ORGANIZATION'S SECURITY POSTURE

Building complex alerts and advanced correlations is not for the faint of heart, but Flow enables you to take on the challenge by making the process more intuitive. You simply drag and drop Flow units into the work area of the visual editor. Units are connected through pipes, which allow the events to flow from one unit to the next, to perform a specific function. Additionally, Flow gives you the flexibility to configure each unit by specifying values, setting additional parameters, and determining notification methods.

With more than 40 units, Flow empowers you to implement a wide range of use cases and gives you the flexibility to customize them to meet your organization's specific needs and risk tolerance. Here are a few use cases that depict how Flow can help strengthen your organization's security posture:

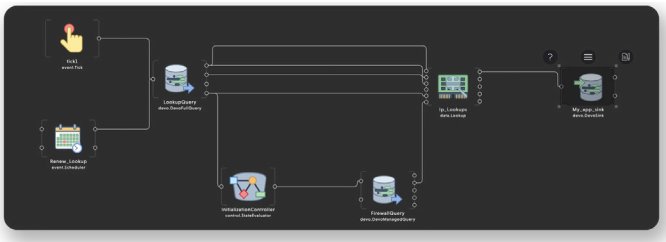
Use Case 1: Limit intruder dwell time with rapid context gathering



With so many tools in the SOC, it can be hard to make sense of the numerous alerts and to pivot from one tool to another to investigate a threat. Flow makes this process easy and speeds up investigations by orchestrating your existing security tools to gather additional context, thus enabling you to determine and mitigate an incident faster.

With Flow, you can send your alerts from a data source, such as an intrusion detection system (IDS), to Devo for deeper analyses and investigation. In this example, once your IDS generates an alert, Flow queries the firewall traffic table to understand the relationship and activities between the victim's IP and the attacker's IP. It will count the number of interactions between these two IP addresses within a specified date range, such as the time the IDS alert triggered until now. If Flow observes a count higher than 1, it will send an email to notify you of the intrusion, and it will provide you with the query to rapidly investigate and mitigate the threat. You can customize the data source, table fields, and the type of notifications based on your organization's tools and preferences.

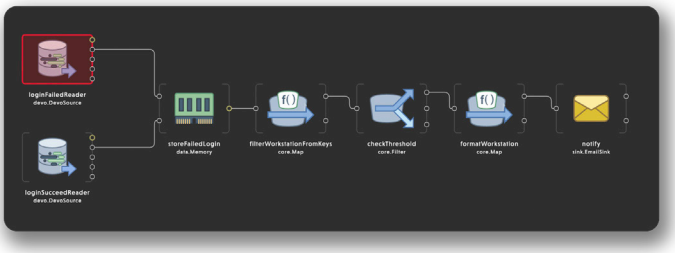
Use Case 2: Automate continuous firewall traffic monitoring to detect threats faster



Flow can help you monitor your security systems at scale by executing on-the-fly enrichments that give you a more granular and combined view from which you can then create detection rules to identify threats.

With Flow, you can monitor all the traffic from your firewall by correlating it against a table in Devo that contains malicious IP addresses. If there is a match, Flow will generate an enriched event that will be logged in a designated table. From this new table, you can take further action by creating detection rules to identify threats that put your organization at risk. You can run this on-the-fly enrichment periodically by configuring the frequency with the scheduler unit.

Use Case 3: Alert after a successful login attempt preceded by numerous failed login attempts



A failed login attempt could mean that an employee forgot their password, but when various failed login attempts precede a successful login attempt, it could mean that an intruder has entered your network. Flow enables you to create a complex alert that involves a sequence of events to notify you of such abnormal behaviors.

With Flow, you could create a complex alert to notify you if a successful login occurred after a specific number of failed login attempts with different usernames from the same IP address to any machine in your network within a determined amount of time. You could configure the number of attempts and the range of time to align it to your organization's risk tolerance.

Are you ready to learn more about Devo Flow?
Contact your sales representative to schedule a demo or visit Devo Docs for more use cases.

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**.