Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

SIEM Integration with Webhooks

Forcepoint

Report

Forcepoint
15 July, 2024
Forcepoint Proprietary

Table of Contents

WEBHOOKS **2**

USING WEBHOOKS IN SIEM SOFTWARE **2**

LOGGING DATA CLASSIFICATION EVENTS WITH PIPEDREAM INTO GOOGLE SHEETS **2**

WORKFLOW 2

RESULT 9

Webhooks

A webhook is a method used in web development to enhance or modify the behavior of a web page or application through custom callbacks. These callbacks are automated messages sent by applications when specific events occur. Triggered by events in a source system, webhooks generate HTTP requests with payload data, which are sent to a destination system. Webhooks enable real-time communication between different applications, allowing them to exchange data seamlessly and synchronize processes. Developers, even if not affiliated with the originating application, can manage, and modify these callbacks. This event-driven communication approach finds applications in various scenarios, enhancing automation and integration between different software systems.

Using Webhooks in SIEM software

Webhooks are used by Security Information and Event Management (SIEM) software to enhance security monitoring and incident response. SIEM tools integrate with webhooks to receive real-time event notifications from various sources, such as authentication systems, cloud services, or other security tools. These notifications trigger automated actions in the SIEM, allowing it to detect and respond to potential security threats promptly. Webhooks provide a seamless way to feed event data into SIEM systems, enhancing threat detection, analysis, and reporting capabilities. This integration enables organizations to achieve more effective and efficient security operations, as SIEM software can aggregate and correlate data from diverse sources to provide a comprehensive view of the security landscape. The result is improved incident response and better protection against cyber threats.

Logging Data Classification events with Pipedream into Google Sheets

Pipedream is an integration platform designed for developers to connect APIs rapidly using a low-code approach. It allows users to create workflows that integrate different applications, data sources, and APIs, without the need for extensive coding. Pipedream facilitates event-driven automations by providing a hosted platform where users can develop and execute workflows that streamline processes and automate tasks. With Pipedream, developers can build efficient connections between numerous services and systems, reducing the need for manual intervention and accelerating development cycles. The platform offers open-source connectors and supports multiple programming languages like Node.js, Python, Go, and Bash. Pipedream simplifies the integration of disparate apps and enables developers to create effective workflows with ease, contributing to enhanced efficiency and productivity in software development.

Workflow
In Connect APIs, AI, databases and more - Pipedream, a workflow is a sequence of steps that automate processes and connect APIs. Workflows make it easy to create and manage integrations, allowing developers to connect different applications, services, and data sources. Workflows consist of steps that are executed in order, and they can include actions, code, and triggers. Triggers define when a workflow is initiated, such as through HTTP requests or scheduled intervals. Each step in a workflow can perform actions like connecting to APIs, manipulating data, and more. Pipedream enables users to create workflows with code-level control when needed, and even offers a no-code approach for automation. Workflows in Pipedream simplify the automation of complex tasks, integration of APIs, and the creation of event-driven processes.

1. Create first Trigger in Pipedream

   Trigger is a fundamental concept that defines the initiation of a workflow. Triggers specify the type of event or condition that starts the execution of a workflow. These events can include HTTP requests, data from external apps or services, scheduled intervals, and more. When a trigger event occurs, the associated workflow is automatically initiated, and the defined steps within the workflow are executed sequentially. For instance, you can set up a trigger to activate a workflow when an HTTP request is received at a specific URL, allowing you to automate actions based on external events. Pipedream's triggers enable developers to create dynamic and event-driven workflows that respond to various inputs and conditions, enhancing automation and integration capabilities.

a) Create your first trigger by using **New HTTP/Webhook Requests** option.

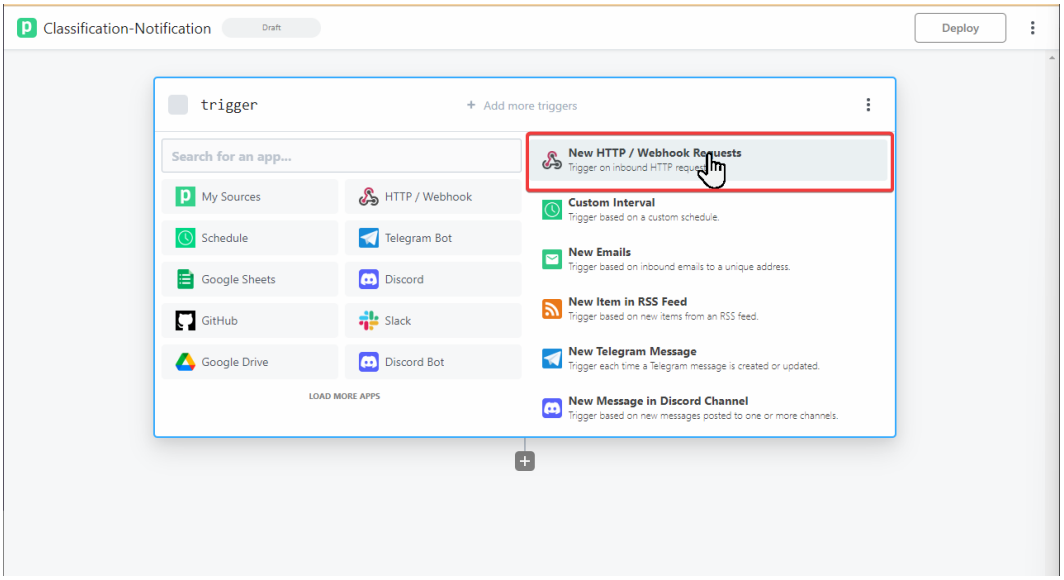


figure 1.

b) Click **Save and Continue** button.

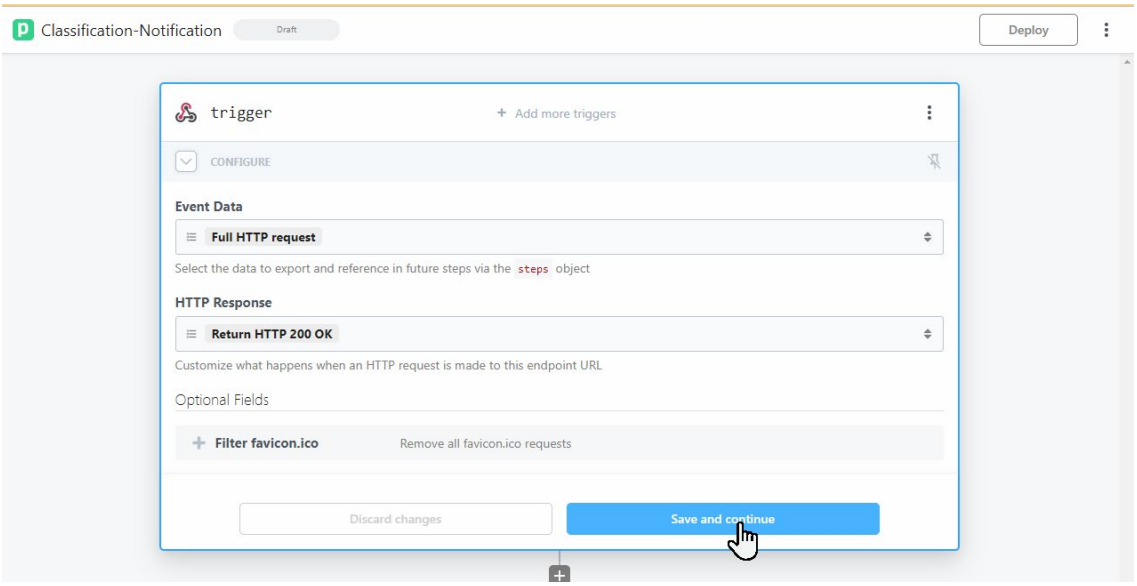


figure 2.

c) Use the newly created URL when configuring a webhook.

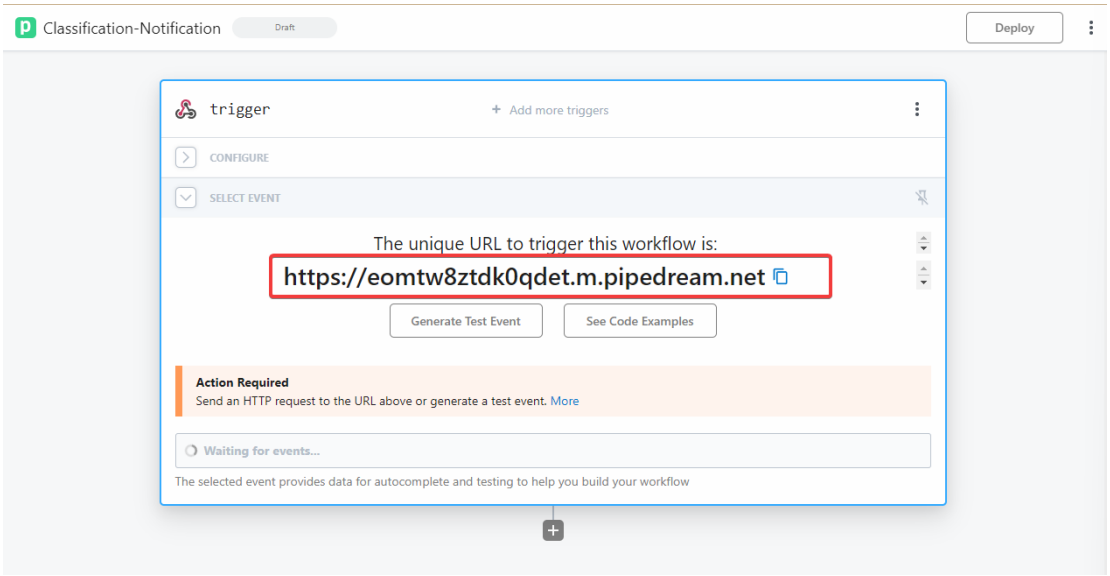


figure 3.

2. Create Webhook in Data Classification

a) Navigate to **Administration > Webhooks**.

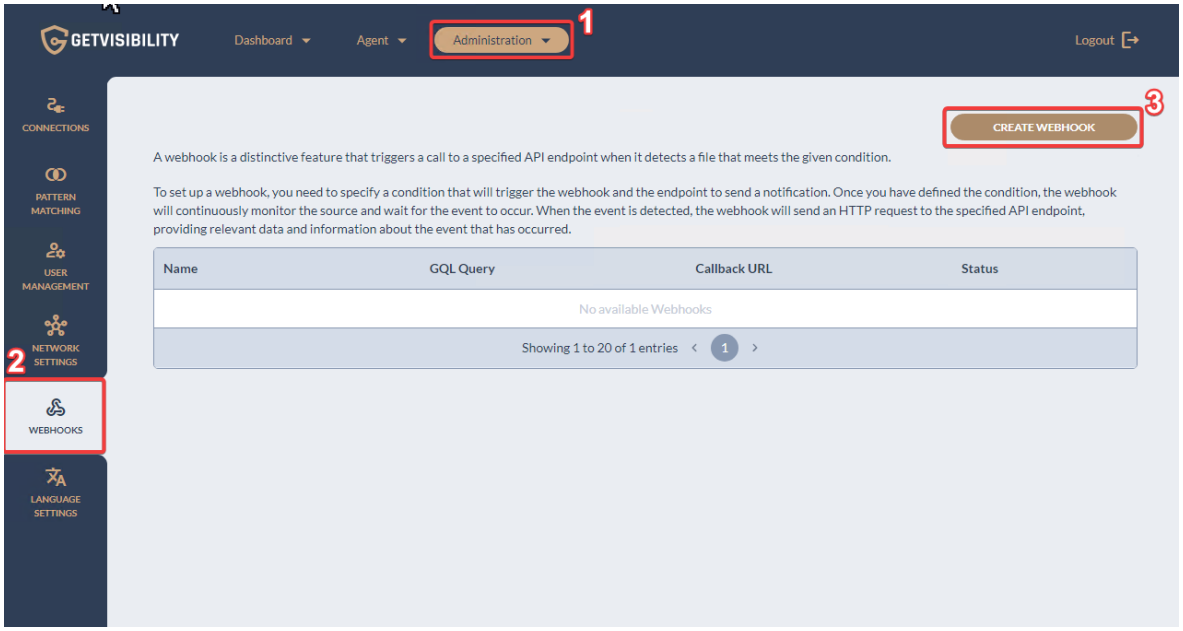


figure 4.

b) To capture classification events, use the "**flow=CLASSIFICATION**" query.

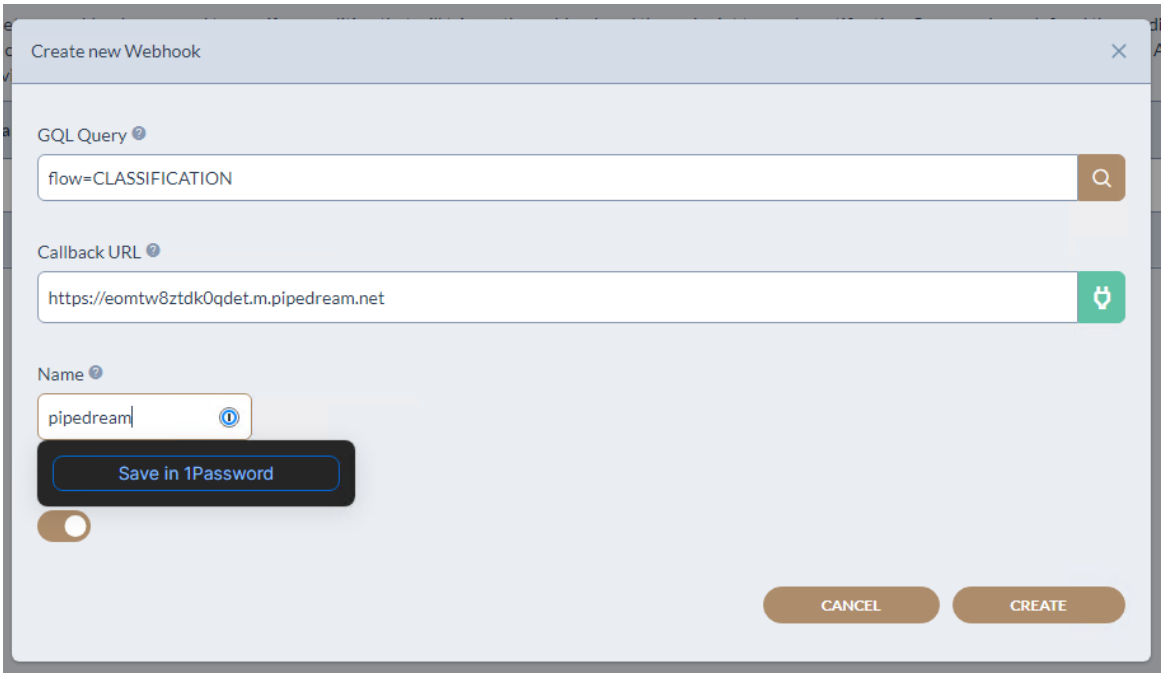


figure 5.

3. Start a scan

   a) Start a previously configured scan, in this example BOX.COM location.

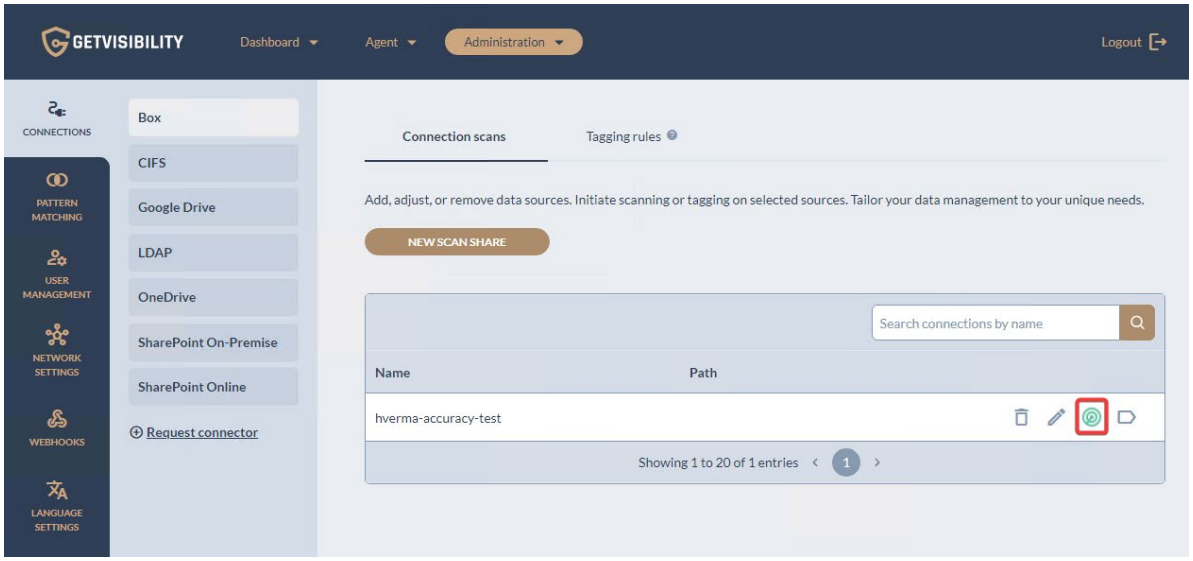


figure 6.

4. An event reached out Pipedream.com!

   a) We can continue with our workflow after first event reach out Pipedream workflow.

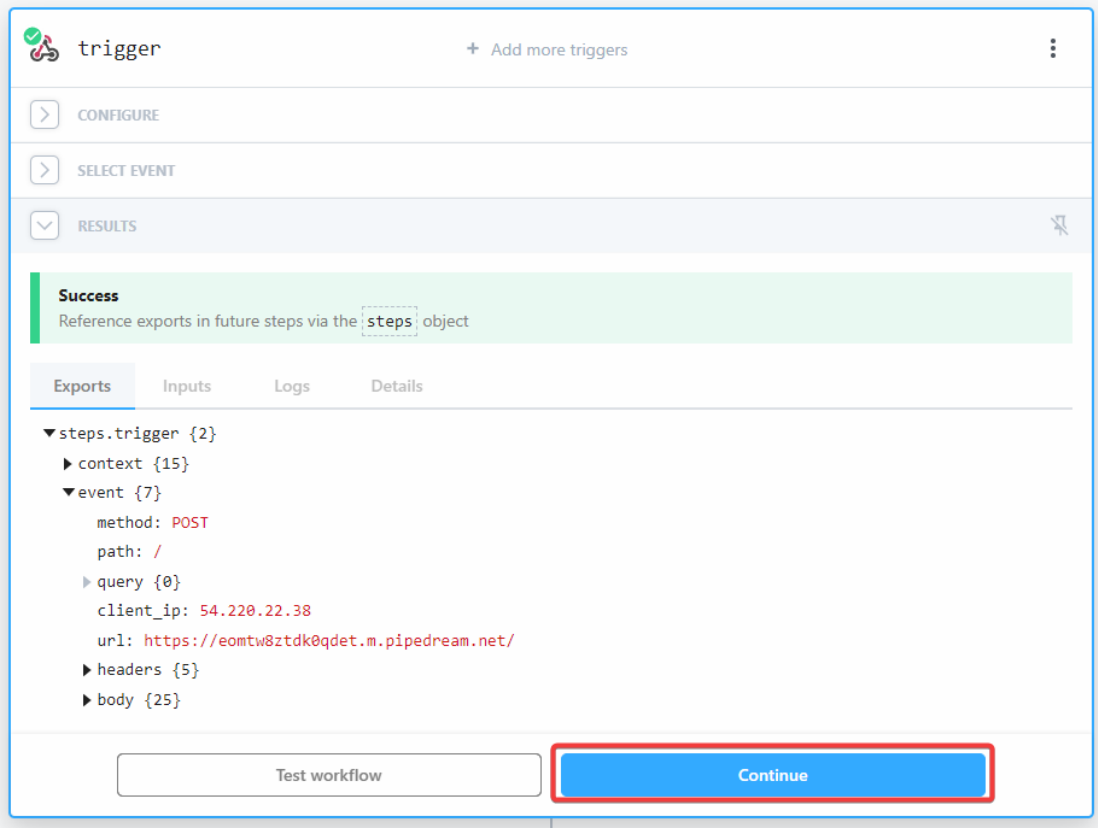


figure 7.

b) After configuring Pipedream to add rows to our test spreadsheet in Google , workflow is completed.

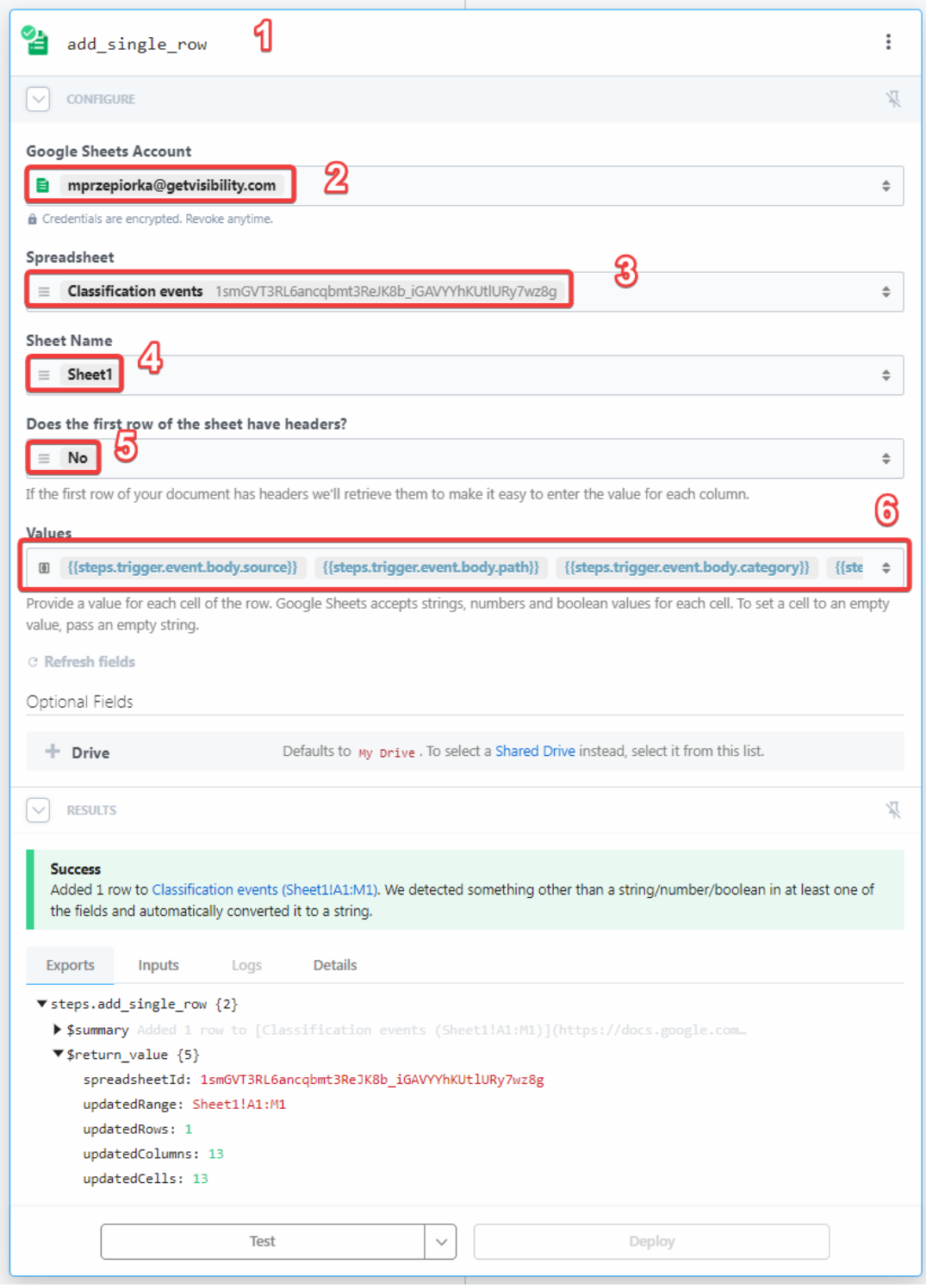


figure 8.

c) Now **Deploy** it and head over to the Sheet to check the action.

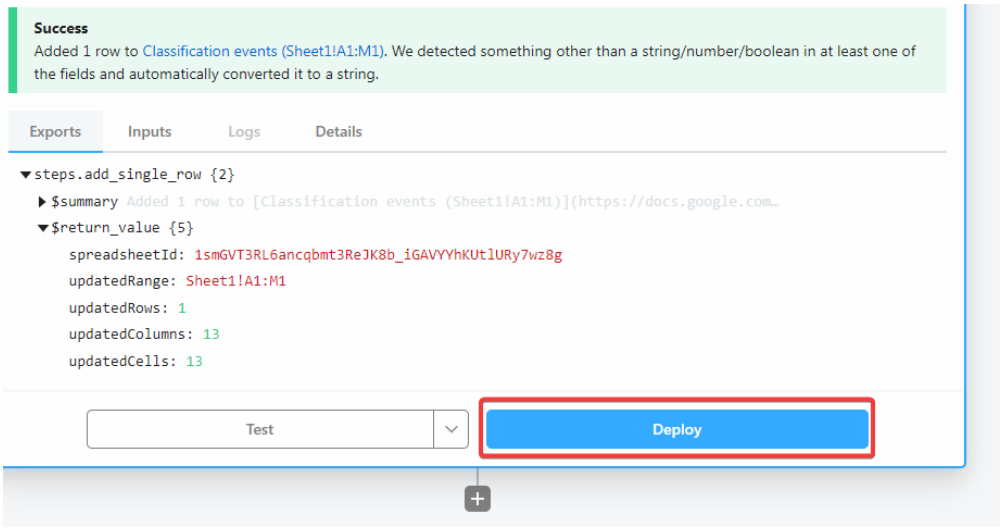


figure 9.

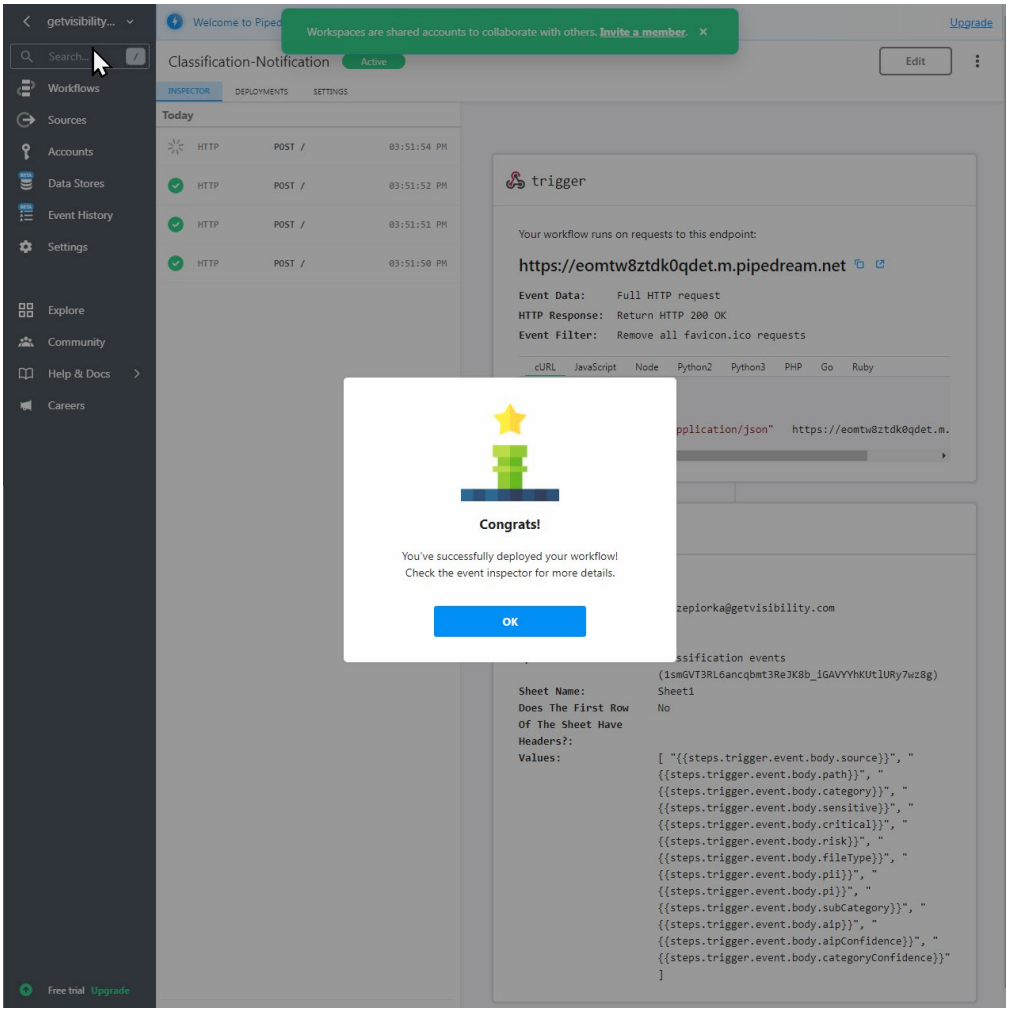
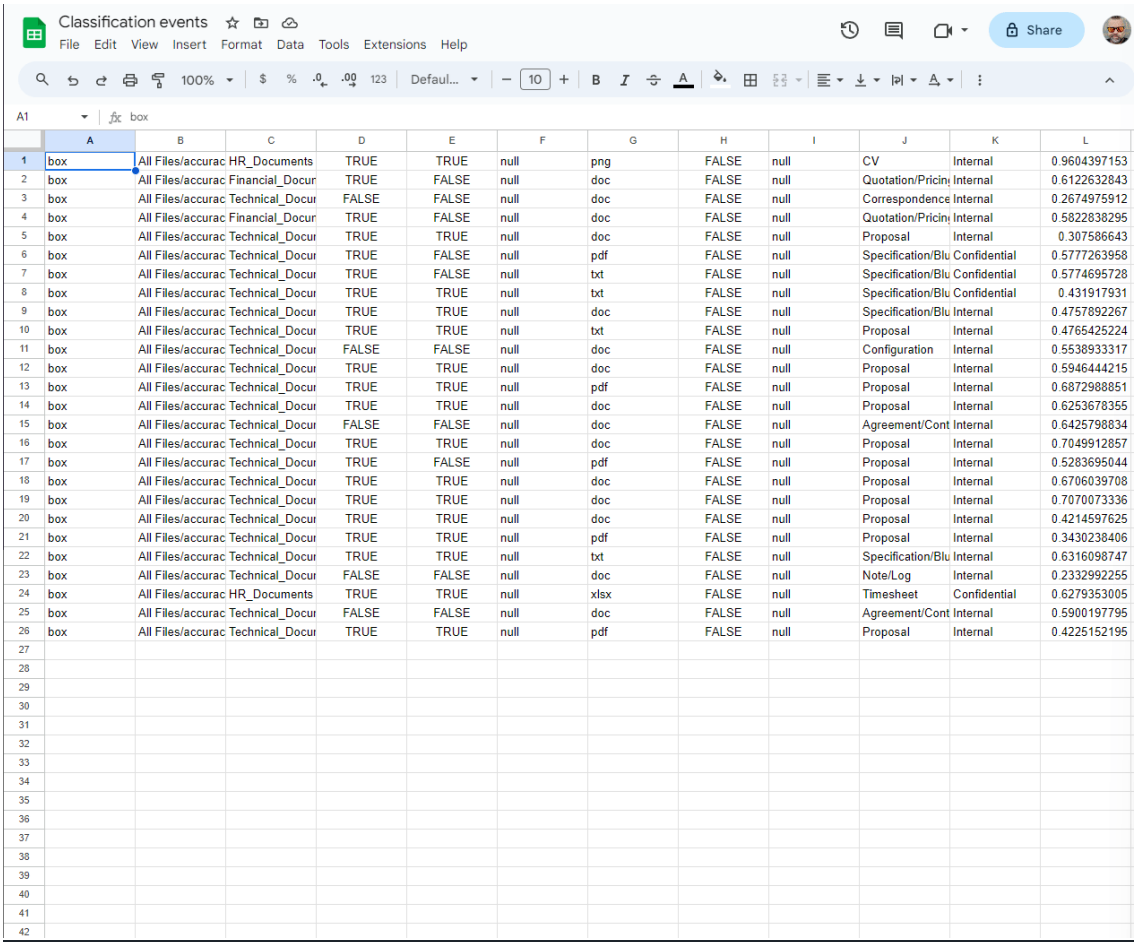


figure 10.

Result

The workflow is now completed and as a result out Sheet is being populated with classification events.



Classification events

File Edit View Insert Format Data Tools Extensions Help

Share

A1 box

	A	B	C	D	E	F	G	H	I	J	K	L
1	box	All Files/accurac	HR_Documents	TRUE	TRUE	null	png	FALSE	null	CV	Internal	0.9604397153
2	box	All Files/accurac	Financial_Docur	TRUE	FALSE	null	doc	FALSE	null	Quotation/Pricin	Internal	0.6122632843
3	box	All Files/accurac	Technical_Docur	FALSE	FALSE	null	doc	FALSE	null	Correspondence	Internal	0.2674975912
4	box	All Files/accurac	Financial_Docur	TRUE	FALSE	null	doc	FALSE	null	Quotation/Pricin	Internal	0.5822838295
5	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.307586643
6	box	All Files/accurac	Technical_Docur	TRUE	FALSE	null	pdf	FALSE	null	Specification/Blu	Confidential	0.5777263958
7	box	All Files/accurac	Technical_Docur	TRUE	FALSE	null	txt	FALSE	null	Specification/Blu	Confidential	0.5774695728
8	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	txt	FALSE	null	Specification/Blu	Confidential	0.431917931
9	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Specification/Blu	Internal	0.4757892267
10	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	txt	FALSE	null	Proposal	Internal	0.4765425224
11	box	All Files/accurac	Technical_Docur	FALSE	FALSE	null	doc	FALSE	null	Configuration	Internal	0.5538933317
12	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.5946444215
13	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	pdf	FALSE	null	Proposal	Internal	0.6872988851
14	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.6253678355
15	box	All Files/accurac	Technical_Docur	FALSE	FALSE	null	doc	FALSE	null	Agreement/Cont	Internal	0.6425798834
16	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.7049912857
17	box	All Files/accurac	Technical_Docur	TRUE	FALSE	null	pdf	FALSE	null	Proposal	Internal	0.5283695044
18	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.6706039708
19	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.7070073336
20	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	doc	FALSE	null	Proposal	Internal	0.4214597625
21	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	pdf	FALSE	null	Proposal	Internal	0.3430238406
22	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	txt	FALSE	null	Specification/Blu	Internal	0.6316098747
23	box	All Files/accurac	Technical_Docur	FALSE	FALSE	null	doc	FALSE	null	Note/Log	Internal	0.2332992255
24	box	All Files/accurac	HR_Documents	TRUE	TRUE	null	xlsx	FALSE	null	Timesheet	Confidential	0.6279353005
25	box	All Files/accurac	Technical_Docur	FALSE	FALSE	null	doc	FALSE	null	Agreement/Cont	Internal	0.5900197795
26	box	All Files/accurac	Technical_Docur	TRUE	TRUE	null	pdf	FALSE	null	Proposal	Internal	0.4225152195

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[Forcepoint Data Classification Powered by Getvisibility SIEM Integration with Webhooks]
[Status]15 Jul. 24