FLARE SYSTEMS + Microsoft

## KEY FEATURES

1 Firework is shipped as Azure Sentinel Solution, delivering a seamless integration

2 Multiple use cases are supported in the Solution (Workbooks, Playbooks, Queries, etc.)

3 The Firework Intelligence Risk Scoring enables an additional layer of prioritization

4 Automation allows straightforward incident creation, response and closure

## FIREWORK FOR MICROSOFT AZURE SENTINEL

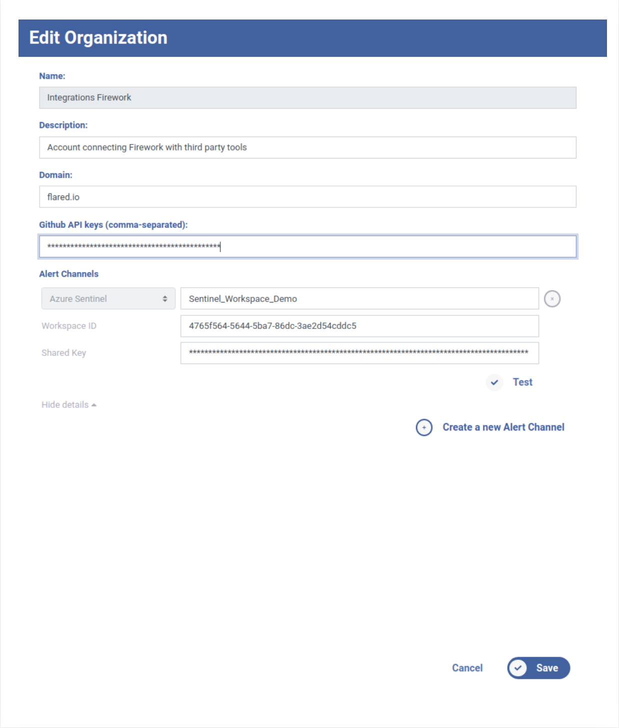
Aggregating logs in a centralized location is a mandatory step for a security team looking to increase their efficiency. Large digital footprint and even greater size of daily logs make any attempts to investigate more than a fraction of all incoming alerts futile. In order to relieve this bottleneck, SIEM and SOAR systems such as Microsoft Azure Sentinel allow to not only aggregate these various logs in a single location, but also to create rules based on heuristics that will allow the automatic creation of incidents, as well as create dashboards and rules when certain thresholds are surpassed.

Connecting your Firework account to Microsoft Azure Sentinel only takes a minute and allows you to send a subset or all of our alerts to your Sentinel instance. Firework is created as an Azure Solution, meaning deploying it through a single click in Azure includes premade dashboards, queries, automated incident creation, update and response through a series of automated actions (Playbooks) that can be enabled to ease the integration and streamline the integration of Firework.

## HOW IT WORKS

On the Firework side, you only need an Azure Workspace ID and a Shared Key to set up an Alert Channel on Firework. From there you will be at liberty of configuring your identifiers (search keywords) to send matching data directly to Sentinel. You can also decide to send critical data only to Sentinel while the rest through regular email or to another system.

Concretely, the Firework platform simply sends data through Azure Sentinel authenticated REST API with data contained in the requested payload. REST API data connectors are configured in Sentinel to write to their own table (Firework_CL in our case) with no requirement regarding the table pre-existing schema; adding columns if they don't exist and leaving blank other fields if incoming data does not have a value for it.



Edit Organization

Name:
Integrations Firework

Description:
Account connecting Firework with third party tools

Domain:
flared.io

Github API keys (comma-separated):
******************************************

Alert Channels

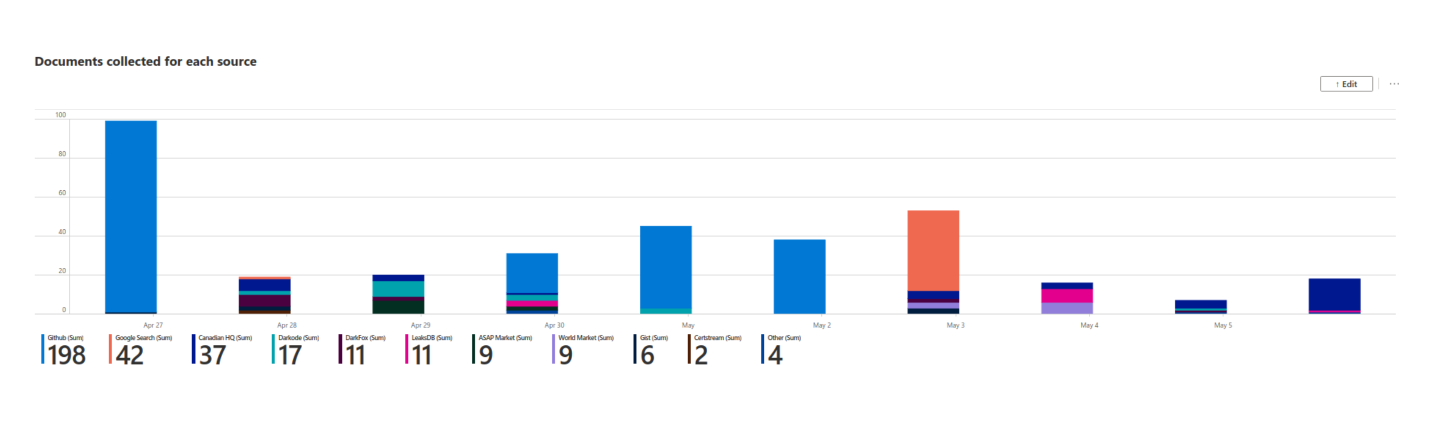
Azure Sentinel | Sentinel_Workspace_Demo

Workspace ID: 4765f564-5644-5ba7-86dc-3ae2d54cddc5

Shared Key: ***********************************************************************************

## AZURE WORKBOOKS AND PLAYBOOKS USE CASES

Firework collects thousands of documents every day, and the prioritization of case reviewing is typically supported by our risk scoring system, helping analysts know where to focus their efforts. With Sentinel playbook and automated incident creation and management, the amount of information that can be analyzed drastically increases.

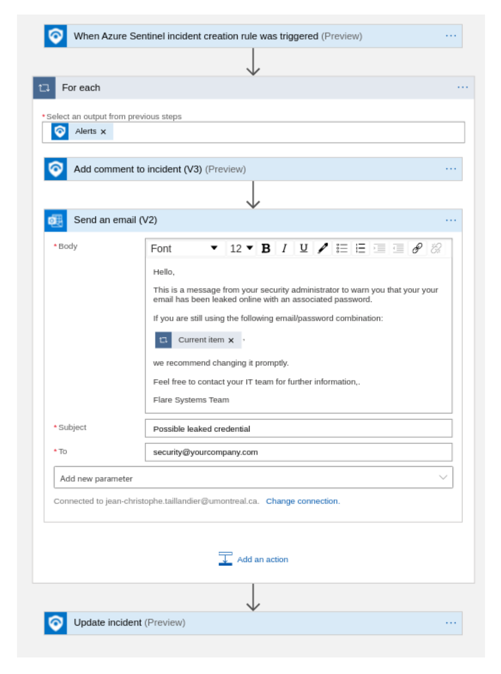


How Azure Sentinel can accelerate Firework's capacity to detect vulnerabilities:

**Fast track analysis of trends in various dark web platforms** by offering real-time analysis and raising alerts or open incidents when necessary. Out of the box analytics and automation rules can show you which platforms are worthy of your attention, and warn you if these change.

**Automate incidents creation and flow to resolve them,** such as email warnings to employees when their credentials are compromised, and closing of the incident when password has been changed.

**Directly integrate your pre-existing systems and processes to Firework.** Avoid having to integrate through API and save precious engineering time.



When Azure Sentinel incident creation rule was triggered (Preview)

For each

* Select an output from previous steps: Alerts

Add comment to incident (V3) (Preview)

Send an email (V2)

* Body:

Hello,

This is a message from your security administrator to warn you that your your email has been leaked online with an associated password.

If you are still using the following email/password combination:

Current item

we recommend changing it promptly.

Feel free to contact your IT team for further information,.

Flare Systems Team

* Subject: Possible leaked credential

* To: security@yourcompany.com

Add new parameter

Connected to jean-christophe.taillandier@umontreal.ca. Change connection.

Add an action

Update incident (Preview)

## ABOUT FIREWORK BY FLARE SYSTEMS

Flare Systems provides solutions to protect your sensitive data. Our AI-driven technology monitors the dark, deep and clear web as well as your digital footprint. It searches for data leaks, and delivers actionable intelligence.

Firework constantly crawls the dark, deep and clear web. It stores, analyzes and structures billions of data points to deliver actionable intelligence through its intuitive platform and API. Firework monitors illicit markets, leaked credentials, technical leaks (API keys, SSH keys, secrets, etc.) and newly-registered domains to detect data breaches caused by human error or by malicious actors to prevent cyber fraud and damage to brand and reputation.