

Flare 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 Flare 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. Flare 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 Flare.

Key Features

- Flare is shipped as Azure Sentinel Solution, delivering a seamless integration
- Multiple use cases are supported in the Solution (Workbooks, Playbooks, Queries, etc.)
- The Flare Intelligence Risk Scoring enables an additional layer of prioritization
- Automation allows straightforward incident creation, response and closure

Edit Organization

Name: Integrations Firewall

Description: Account connecting Firewall with third party tools

Domain: flare.io

GitHub API keys (comma-separated):

Alert Channels

Azure Sentinel Sentinel_Workspace_Demo

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

Shared Key: [Redacted]

Test

Hide details

Create a new Alert Channel

Cancel Save

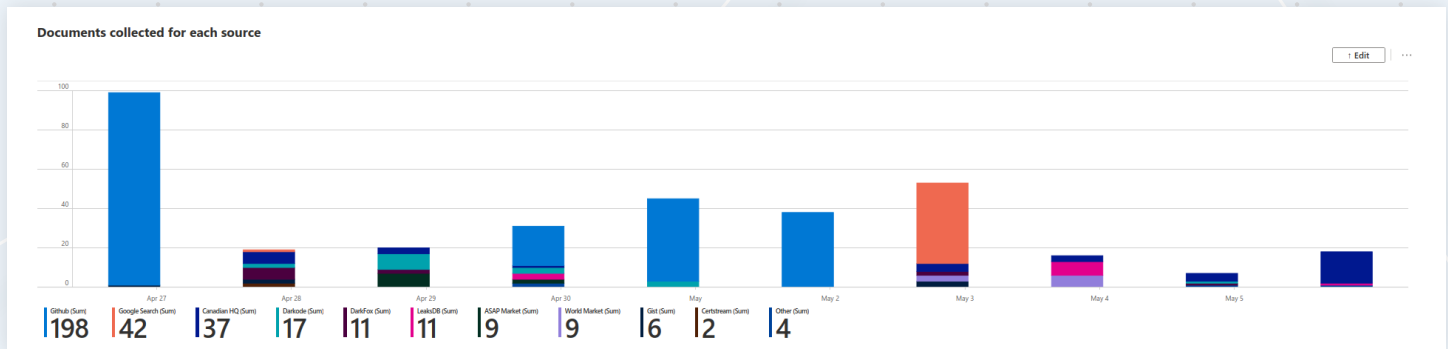
How it Works

On the Flare side, you only need an Azure Workspace ID and a Shared Key to set up an Alert Channel on Flare. 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 Flare 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 (Flare_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.

Azure Workbooks And Playbooks Use Cases

Flare 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.

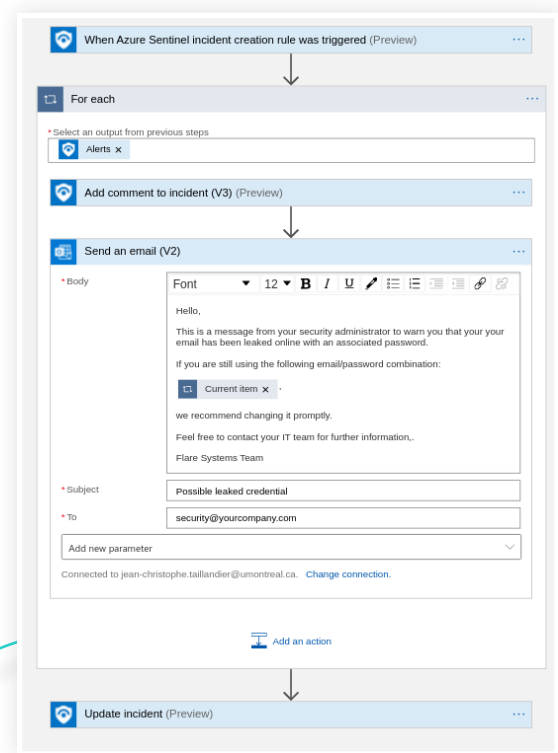


How Azure Sentinel can accelerate Flare's capacity to detect vulnerabilities:

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 Flare. Avoid having to integrate through API and save precious engineering time.



About Flare

Flare 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.

Flare 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. Flare 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.