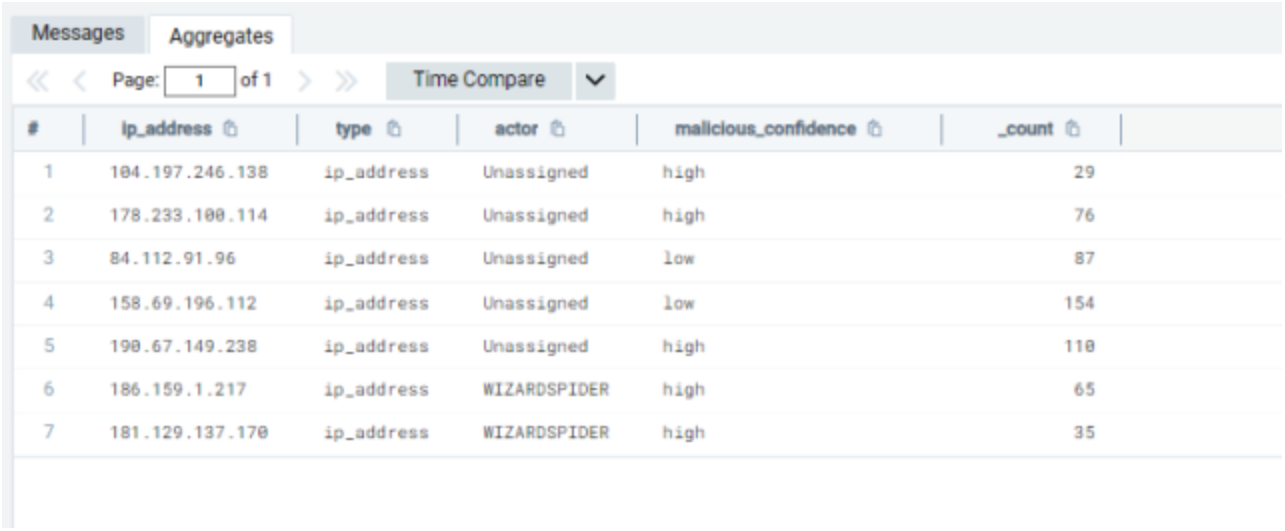
Sumo Logic – Querying CrowdStrike Threat Intelligence

dev.classmethod.jp/articles/sumo-logic-crowdstrike-threat-intel

佐久間昇吾

October 24, 2023



Messages | Aggregates

Page: 1 of 1 | Time Compare

#	ip_address	type	actor	malicious_confidence	_count
1	104.197.246.138	ip_address	Unassigned	high	29
2	178.233.100.114	ip_address	Unassigned	high	76
3	84.112.91.96	ip_address	Unassigned	low	87
4	158.69.196.112	ip_address	Unassigned	low	154
5	190.67.149.238	ip_address	Unassigned	high	110
6	186.159.1.217	ip_address	WIZARDSPIDER	high	65
7	181.129.137.170	ip_address	WIZARDSPIDER	high	35

Sumo Logic imports CrowdStrike threat data into its database. By matching and searching this threat data against log data, malicious attacks can be detected. There are two main ways to use this threat information:

One is to create a dashboard to understand threats and trends. I have blogged about this in the past. Sumo Logic – Creating a CrowdStrike Threat Detection Dashboard | DevelopersIO

This time, we will take a closer look at the above mechanism and explain the second way to use it: how actual queries are created.

Searching for threat information using the threatip and lookup operators

There are two ways to search threat information by query:

The first is to use **the threatip operator** , which is the easiest way to leverage CrowdStrike's threat intelligence to search your logs for IP addresses commonly used by malicious actors or groups.

Second, using **the lookup operator , you can leverage all of Sumo Logic's CrowdStrike threat intelligence to find matches to malicious IP addresses, URLs, domains, hash 256s, and emails.**

Let's look at how to write a query step by step.

How to use the threatip operator

The operator threatip is given the field containing the IP address as an argument.

syntax

```
| threatip "ipアドレスのフィールド"
```

This outputs the following data:

- **actor**
  Attacker name
  *Unassigned corresponds to a threat, but the attacker name is unknown or has not yet been assigned.
- **malicious_confidence**
  Importance
- **raw_threat**
  Shows which part of the log contains the IP address
- **type**
  threatip operator displays ip_address

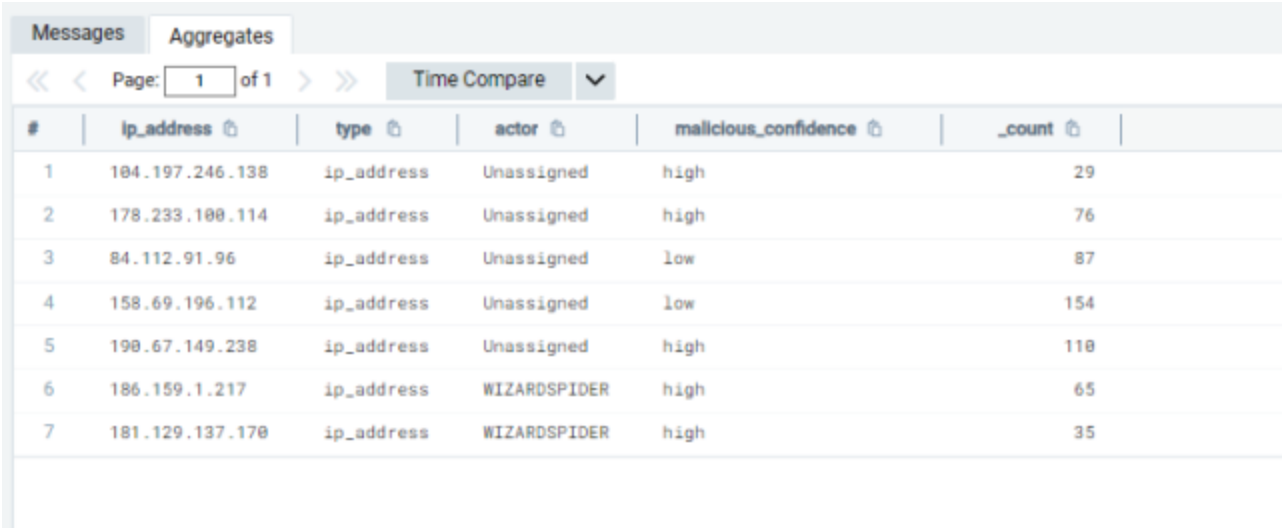
Now, let's search in a demo environment and see the output results.

Search query content

```
_sourceCategory=Labs/Apache/Access
| parse regex "(?<ip_address>\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| threatip ip_address
| where !(isNull(malicious_confidence))
| count by ip_address, type, actor, malicious_confidence
```

Line 1: Searches Apache web server access logs.
Line 2: By adding the optional regex to the parse operator, IP address data is extracted from the ip_address field using the regular expression \b\d{1,3}.
Line 3: Matches CrowdStrike threat information with the ip_address field.
Line 4: Outputs search results where malicious_confidence is not null. (The where operator filters the search results. isNull checks whether the string in the malicious_confidence field is null. ! is used to specify the negative form.) Line 5: Aggregates by ip_address, type, actor, and malicious_confidence.

Search Results



#	ip_address	type	actor	malicious_confidence	_count
1	104.197.246.138	ip_address	Unassigned	high	29
2	178.233.100.114	ip_address	Unassigned	high	76
3	84.112.91.96	ip_address	Unassigned	low	87
4	158.69.196.112	ip_address	Unassigned	low	154
5	190.67.149.238	ip_address	Unassigned	high	110
6	186.159.1.217	ip_address	WIZARDSPIDER	high	65
7	181.129.137.170	ip_address	WIZARDSPIDER	high	35

This will allow you to search so that only logs that have been flagged by CrowdStrike's threat information are output. If the search results are output like this, drill-down and correlation analysis will be required to understand the attacker's traces, intrusion route, and depth of the attack. This is where you'll want to expand your investigation methods using dashboards and queries, and set up alerts for detection in case of an emergency.

How to use CrowdStrike threat intelligence with lookup operators

Next is the lookup operator, which searches for data from lookup tables stored in Sumo Logic and uses them for searches. One of the lookup tables stored in Sumo Logic contains threat information from CrowdStrike, and this data is matched with logs to perform searches.

syntax

```
| lookup "ルックアップテーブルから抽出するフィールド名" from "ルックアップテーブル名" on "照合先のルックアップテーブルのフィールド名"="照合元のログのフィールド名"
```

The data output by this is as follows (some of the data will be output differently than when using the threatip operator):

- **actor**
  Attacker name
  *Unassigned corresponds to a threat, but the attacker name is unknown or has not yet been assigned.

- **threatlevel**
  Importance *Unverified means the importance is unknown or has not yet been assigned.

- **raw**

Displays which part of the log contains information relevant to the threat

- **type**
  Shows ip_address, domain, email_address, hash_sha256, url

- **threat**
  Base threat information such as IP addresses and URLs belonging to the above types

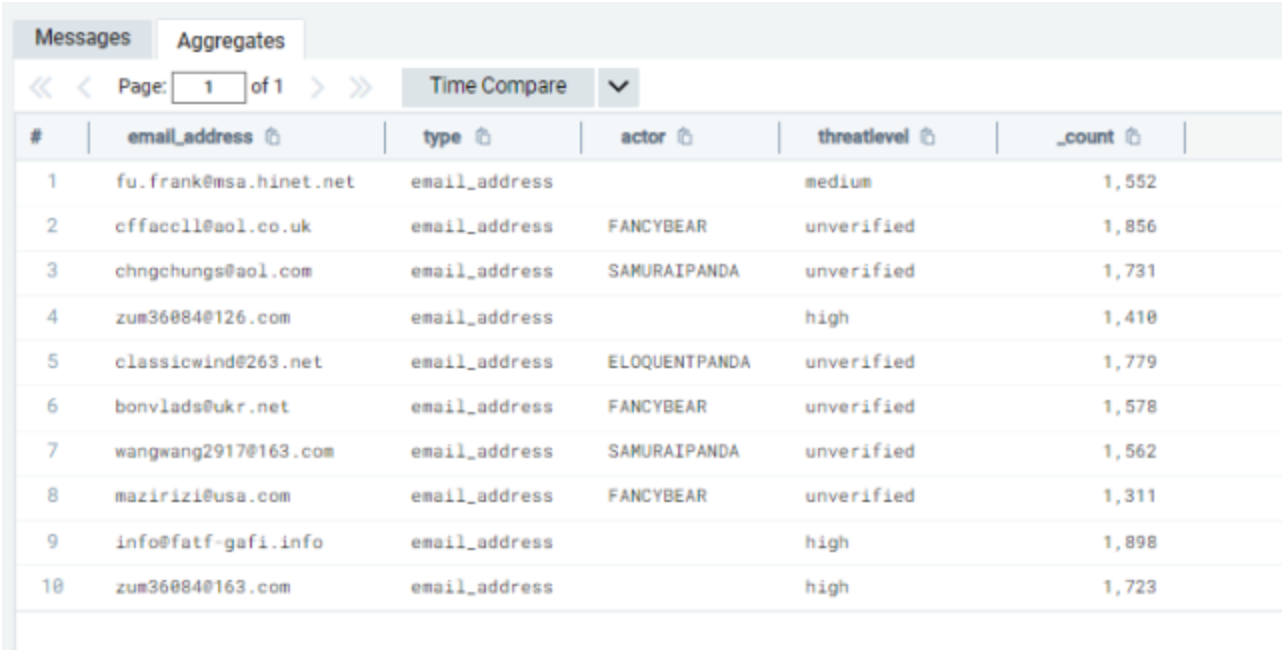
Now, let's search in a demo environment and see the output results.

Search query content

```
_sourceCategory=Labs/TravelApp
| parse regex "(?<email_address>[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[a-zA-Z]{2,4})"
| lookup type, actor, threatlevel from sumo://threat/cs on threat=email_address
| where !(isNull(threatlevel))
| count by email_address, type, actor, threatlevel
```

Lines 1 and 2: Same as above. The regular expression and field names for parse regex have been changed for email addresses.
Line 3: The field names to extract from the lookup table are specified as type, actor, and threatlevel. The lookup table name is sumo://threat/cs, which specifies the CrowdStrike table. threat=email_address checks whether the email address in the lookup table called threat matches the email_address field extracted from the log.
Line 4: Outputs search results where threatlevel is not null. (The search results are filtered using the where operator. isNull checks whether the string in the threatlevel field is null. The ! is used to specify the negative form.)
Line 5: Aggregates by email_address, type, actor, and threatlevel

Search Results



#	email_address	type	actor	threatlevel	_count
1	fu.frank@msa.hinet.net	email_address		medium	1,552
2	cffaccll@aol.co.uk	email_address	FANCYBEAR	unverified	1,856
3	chngchungs@aol.com	email_address	SAMURAIPANDA	unverified	1,731
4	zum360840126.com	email_address		high	1,410
5	classicwind@263.net	email_address	ELOQUENTPANDA	unverified	1,779
6	bonvlads@ukr.net	email_address	FANCYBEAR	unverified	1,578
7	wangwang2917@163.com	email_address	SAMURAIPANDA	unverified	1,562
8	mazirizi@usa.com	email_address	FANCYBEAR	unverified	1,311
9	info@fatf-gafi.info	email_address		high	1,898
10	zum360840163.com	email_address		high	1,723

As you can see, if an actor is not assigned, it will not be output, so it is a good idea to filter by threatlevel (severity) using where. Also, since attackers are just as concerned about the threatlevel as defenders, it is quite possible that they will change IP addresses, email addresses, etc., so we recommend checking the threatlevel even if it is displayed as Medium or Low.

Below are various regular expressions that you can use depending on your needs.

```
// ip_address
| parse regex "(?<ip_address>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
// url
| parse regex "(?<url>(?:http(?:s)?:\/\/.)?(?:www\.)?[-a-zA-Z0-9@:%._\+~#=]{2,256}\.
[a-z]{2,6}\b(?:[-a-zA-Z0-9@:%_\+.~#?&//=]*))"
// email_address
| parse regex "(?<email_address>[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[a-zA-Z]{2,4})"
// hash_256
| parse regex "(?<hash_256>\b[A-Fa-f0-9]{64}\b)"
// domain
| parse regex "(?<domain>\b[a-zA-Z0-9][a-zA-Z0-9-_]{1,61}[a-zA-Z0-9]\.[a-zA-Z]{2,6}|
[a-zA-Z0-9-]{2,30}\.[a-zA-Z]{2,3}\b)"
```

*If the log is in json format, Auto ParseMode will work, so the above is not necessary.

summary

This time, we showed you how to write queries using CrowdStrike threat information that can be detected by Sumo Logic! If you are detecting threats using other security products (EDR, WAF, DLP, etc.), you can also use similar queries to search logs and visualize them using dashboards to improve your ability to track attack traces and clarify your investigation methods.

I hope this information will be of some help to you.