Network Security Project

Log Analysis

Instructor: Shiuhpyng Shieh

TA: Yung-Hao Li, Pin-Ching Chen, Tsung-Sheng Wang

Due date: 23:55, May 31, 2022

Project Description

- 3 scenarios in total, each student will be assigned a scenario.
    - Attack scenarios are described in spec
- Logs are collected with Windows Event, Sysmon, and Zeek.
- Report (100%)
    - Indicator of Compromise (IoC) (50%)
        - E.g. IP address, etc.
    - Detailed timeline of the attack (20%)
        - TAs will specify which behavior should be plotted on the timeline.
    - Possible detection method (20%)
    - Feedback (10%)

Objective

- Identify malicious traces from raw logs.
- Become familiar with commonly used data source.
- Identify potential threats through log analysis.

Introduction to Windows Event / Sysmon

- Windows events are shown in the Windows Event Viewer.
- The Windows Event Viewer shows a log of application and system messages, including errors, information messages, and warnings. [2]
  - It's a useful tool for troubleshooting all kinds of different Windows problems.
- System Monitor (Sysmon) is a Windows system service and device driver that monitor and log system activity to the Windows event log. [3]
  - It provides detailed information about process creations, network connections, and changes to file creation time.

[2] https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/
[3] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Introduction to Bro

- Bro is an open-source network security monitoring tool that observes network traffic.
- Bro interprets what it sees and creates compact, high-fidelity transaction logs, file content, and fully customized output, suitable for manual review on disk or in a more analyst-friendly tool like a security and information event management (SIEM) system. [4]
- The new name: Zeek

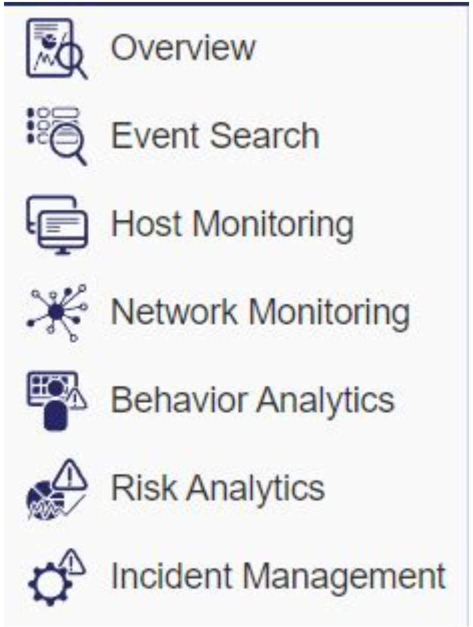
[4] https://zeek.org/

Visualizing logs

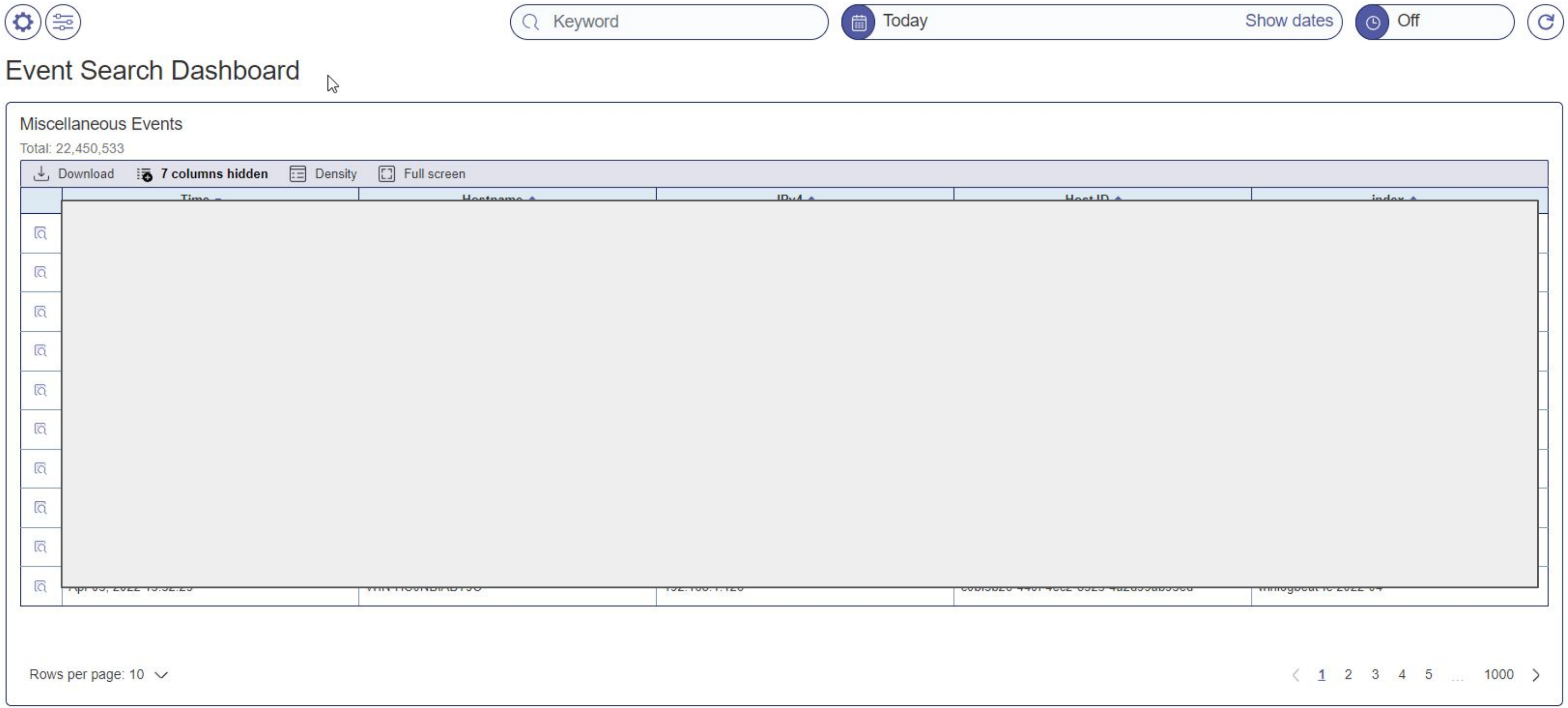
- Woodpecker platform: https://woodpecker.dsns.cs.nycu.edu.tw/xvr/login
  - Username: user
  - Password: netsecstudent2022

- The event occurred on Mar 31, please make sure you specify the date so that you are able to see the logs.

Woodpecker Tutorial - Sidebar



Event Search

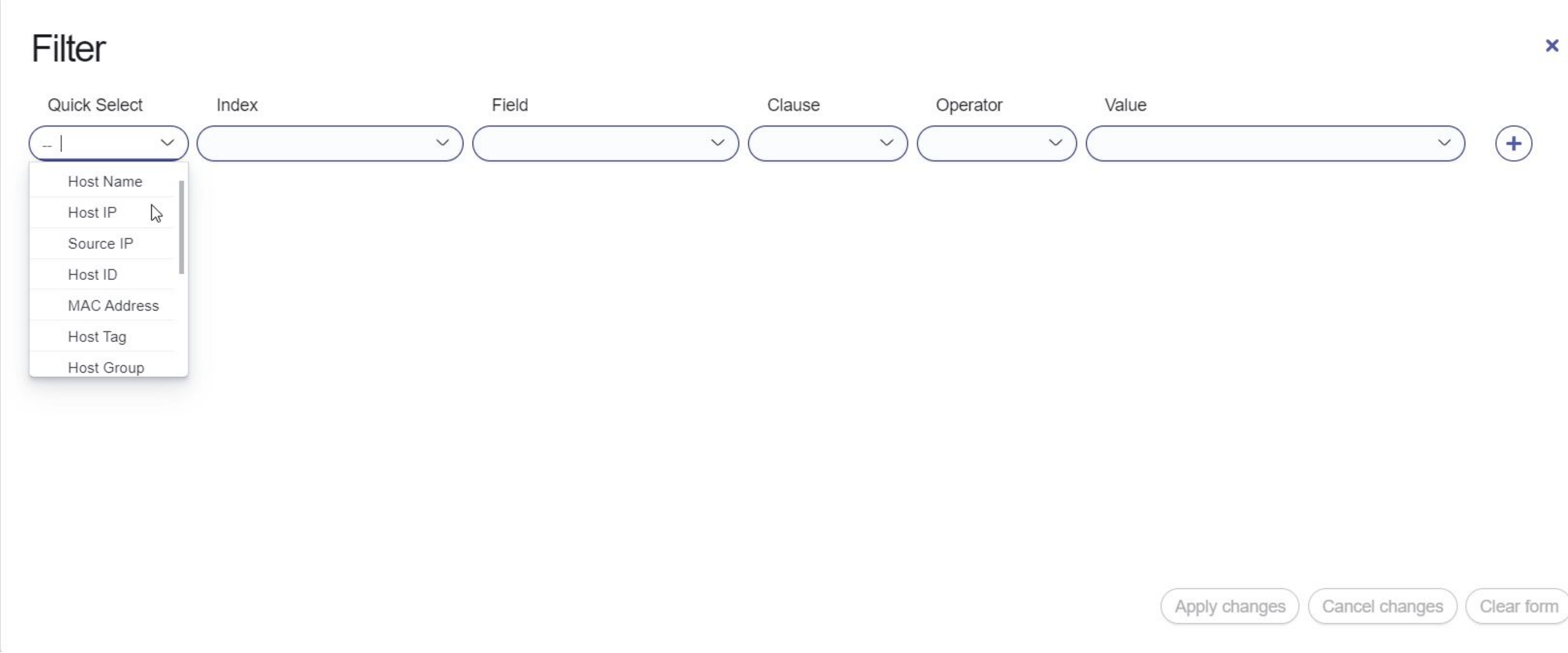


Event Search Dashboard

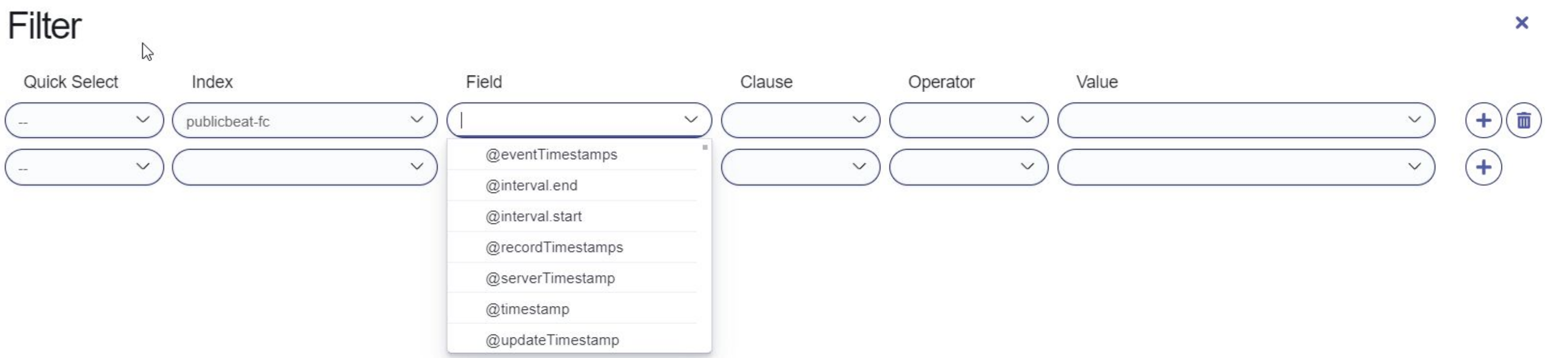
Miscellaneous Events

Total: 22,450,533

Filter

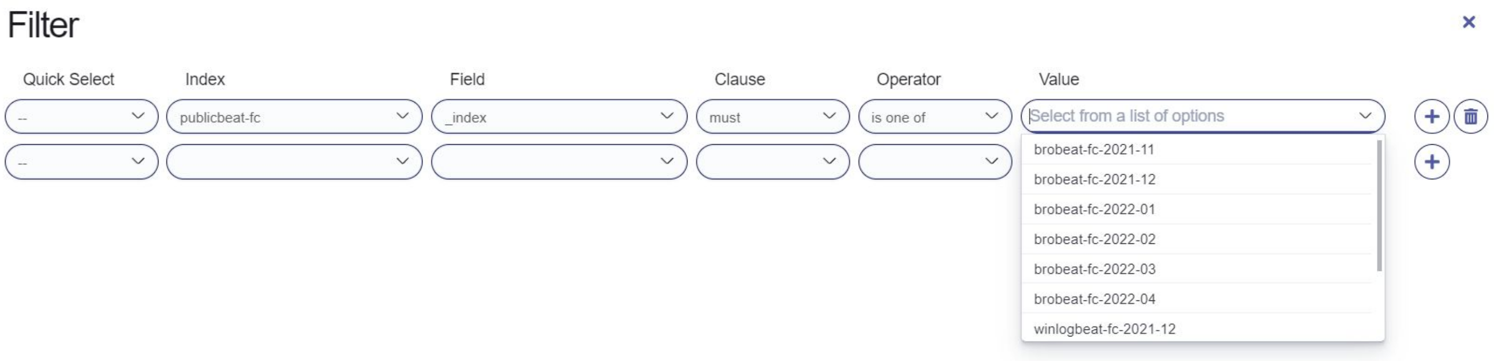


Filter
×
Quick Select
Index
Field
Clause
Operator
Value
--
Host Name
Host IP
Source IP
Host ID
MAC Address
Host Tag
Host Group
+
Apply changes
Cancel changes
Clear form



Filter

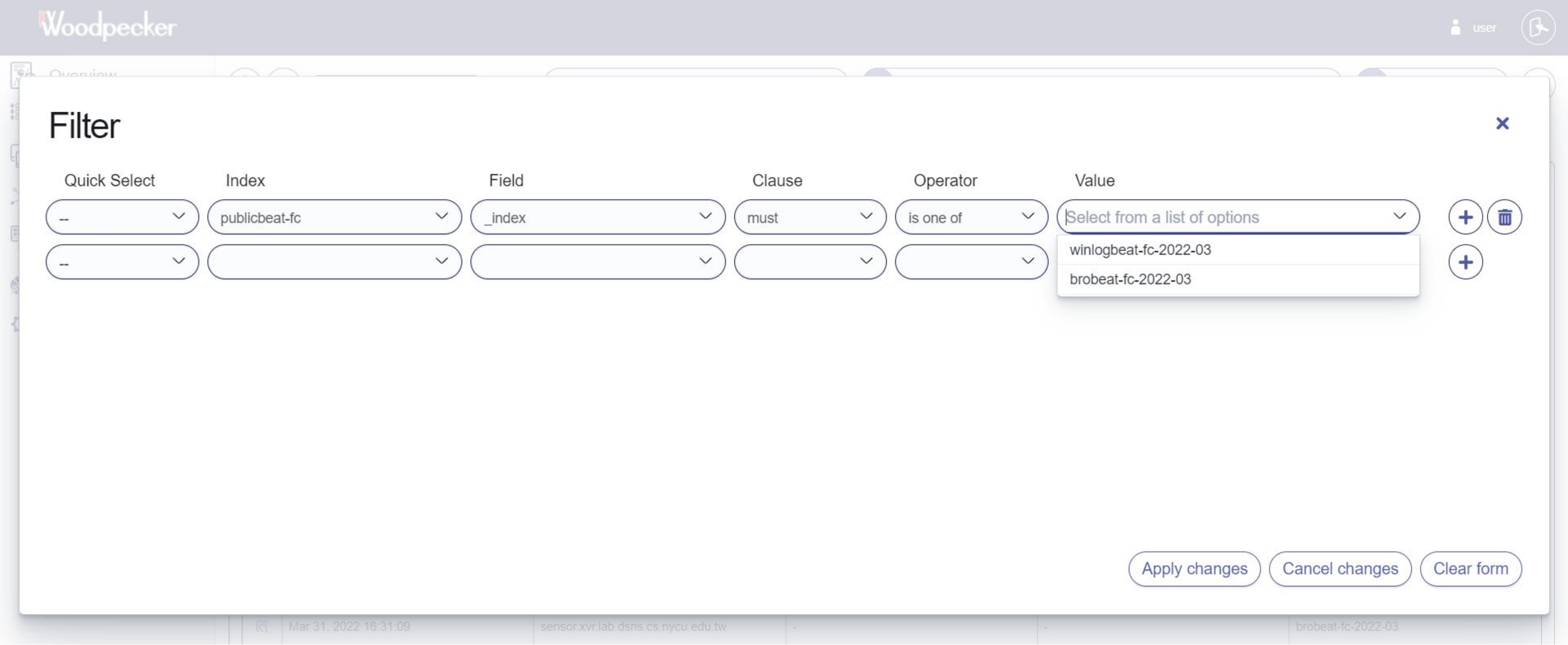
Quick Select: --
Index: publicbeat-fc
Field:
Clause:
Operator:
Value:



Filter

Quick Select: --
Index: publicbeat-fc
Field: _index
Clause: must
Operator: is one of
Value: Select from a list of options

2 index (winlogbeat / brobeat)

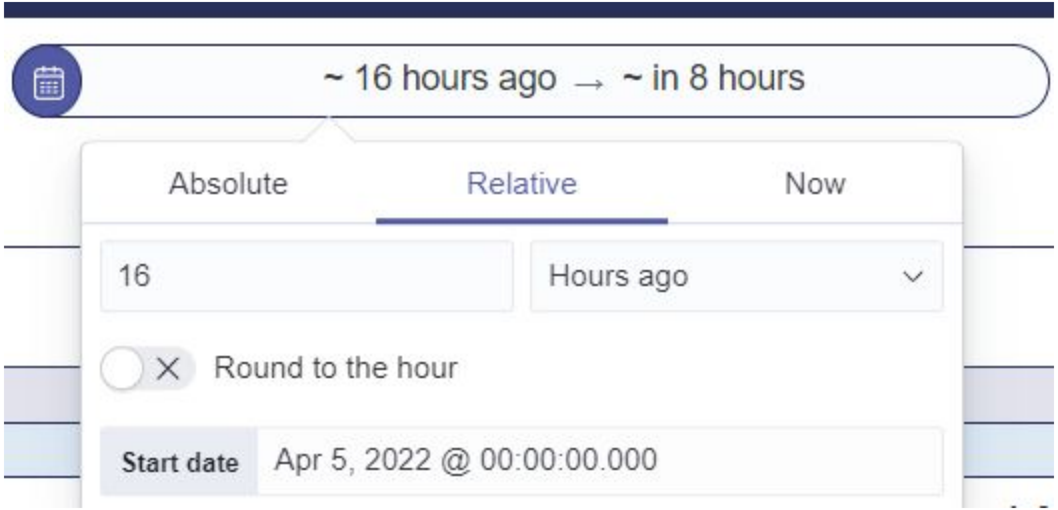


Quick Select	Index	Field	Clause	Operator	Value
--	publicbeat-fc	_index	must	is one of	Select from a list of options
--					

winlogbeat-fc-2022-03

brobeat-fc-2022-03

Time picker



~ 16 hours ago → ~ in 8 hours

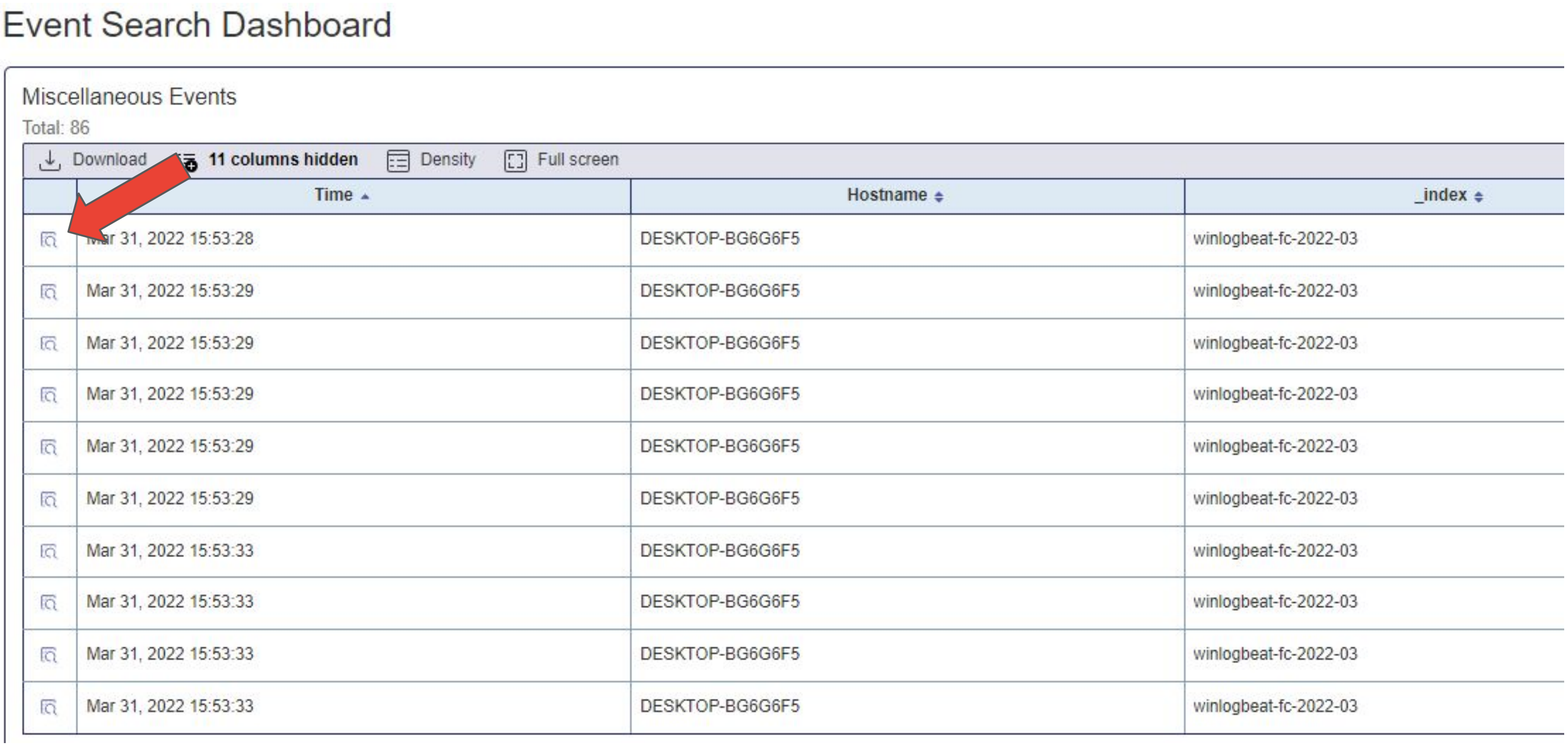
16

Hours ago

Round to the hour

Start date: Apr 5, 2022 @ 00:00:00.000

log detail



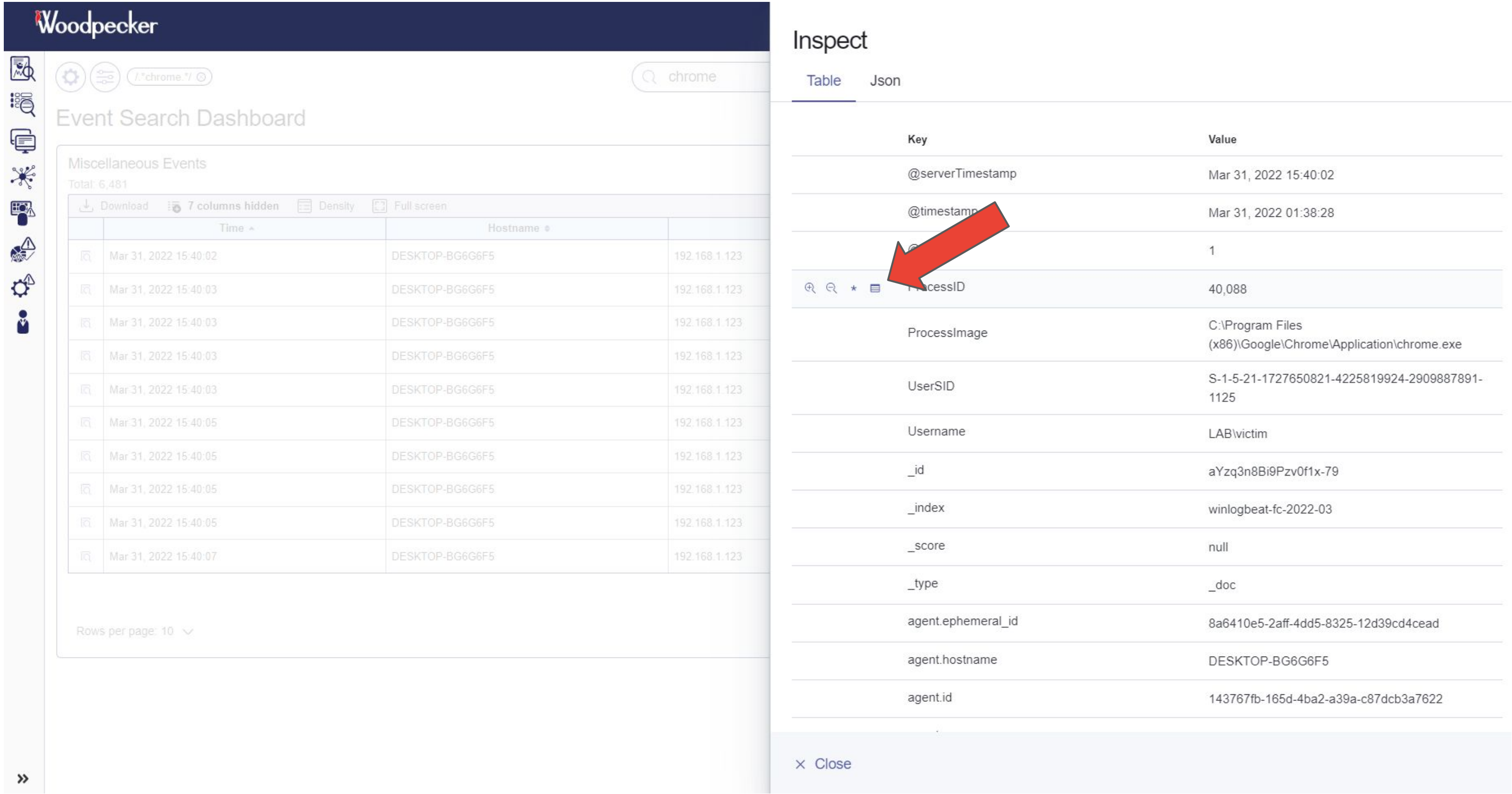
Event Search Dashboard

Miscellaneous Events

Total: 86

	Time	Hostname	_index
	Mar 31, 2022 15:53:28	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:29	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:29	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:29	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:29	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:29	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:33	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:33	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:33	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03
	Mar 31, 2022 15:53:33	DESKTOP-BG6G6F5	winlogbeat-fc-2022-03

Add column



Woodpecker

/.*chrome.*/

chrome

Event Search Dashboard

Miscellaneous Events

Total: 6,481

Download | 7 columns hidden | Density | Full screen

Time	Hostname	
Mar 31, 2022 15:40:02	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123
Mar 31, 2022 15:40:07	DESKTOP-BG6G6F5	192.168.1.123

Rows per page: 10

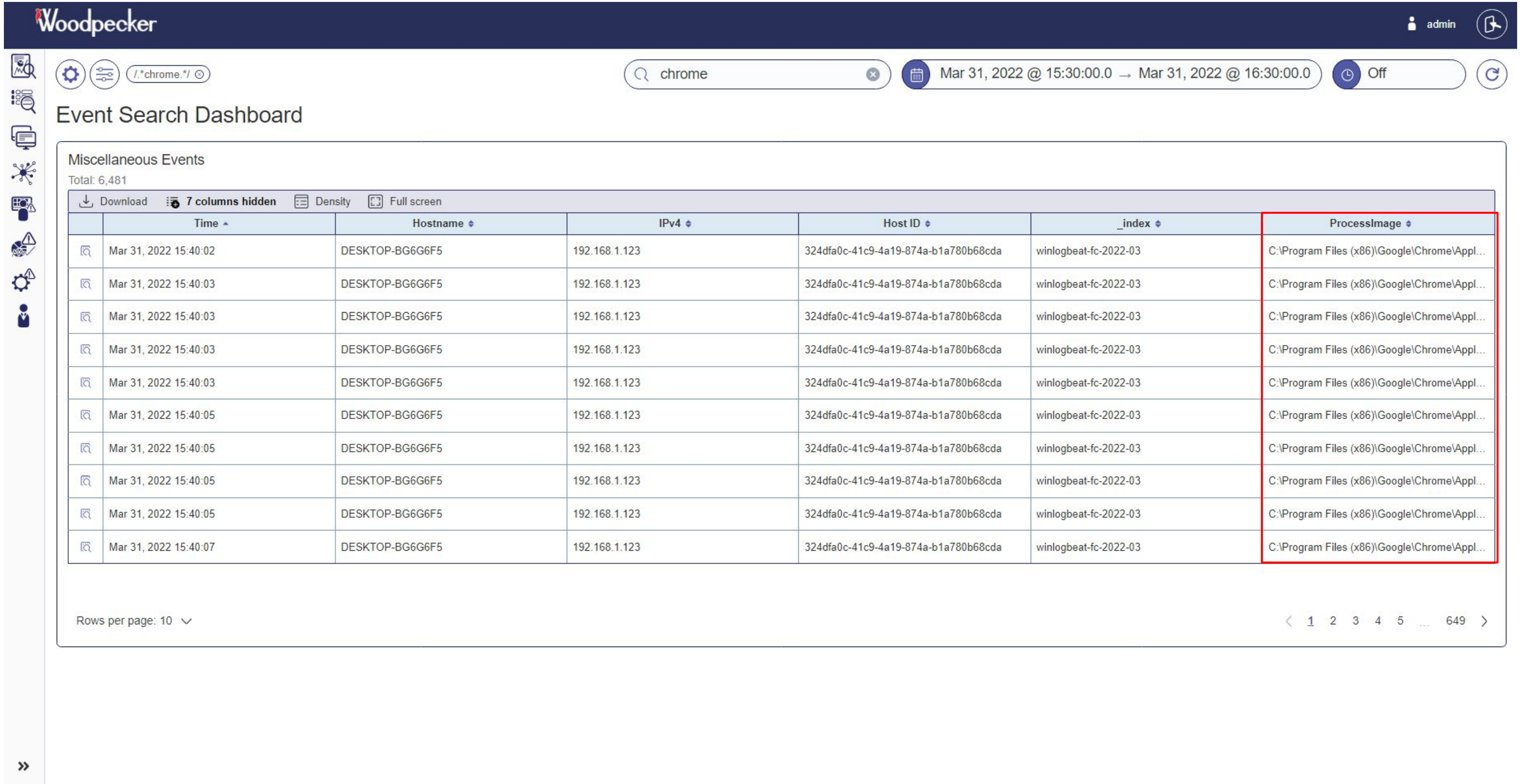
Inspect

Table | Json

Key	Value
@serverTimestamp	Mar 31, 2022 15:40:02
@timestamp	Mar 31, 2022 01:38:28
@	1
ProcessID	40,088
ProcessImage	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
UserSID	S-1-5-21-1727650821-4225819924-2909887891-1125
Username	LAB\victim
_id	aYzq3n8Bi9Pzv0f1x-79
_index	winlogbeat-fc-2022-03
_score	null
_type	_doc
agent.ephemeral_id	8a6410e5-2aff-4dd5-8325-12d39cd4cead
agent.hostname	DESKTOP-BG6G6F5
agent.id	143767fb-165d-4ba2-a39a-c87dcb3a7622

× Close

New column



chrome

Mar 31, 2022 @ 15:30:00.0 → Mar 31, 2022 @ 16:30:00.0

Event Search Dashboard

Miscellaneous Events

Total: 6,481

	Time	Hostname	IPv4	Host ID	_index	ProcessImage
	Mar 31, 2022 15:40:02	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:03	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:05	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...
	Mar 31, 2022 15:40:07	DESKTOP-BG6G6F5	192.168.1.123	324dfa0c-41c9-4a19-874a-b1a780b68cda	winlogbeat-fc-2022-03	C:\Program Files (x86)\Google\Chrome\Appl...

Rows per page: 10

< 1 2 3 4 5 ... 649 >

Hint

- winlog beat
  - event.code: 1, 3, 11, 4625
  - ProcessImage

- brobeat
  - id_resp.p, id_resp.h
  - id_orig.p, id_orig.h