LOGPOINT

Integrations

Cybereason

V5.1.0 (latest)

CONTENTS

CHAPTER ONE

CYBEREASON

Cybereason enables you to fetch and analyze *Cybereason Malops* and *Cybereason Malware Query* logs. It identifies malicious operations (Malops) in real-time and provides detailed insights into the attack, including the attack's timeline, affected users and the root cause.

Cybereason Components

1. **Universal REST API Fetcher**
    - CybereasonFetcher
2. **Compiled Normalizer**
    - CybereasonCompiledNormalizer
3. **Search Template**
    - LP_CybeReason MalOps

CHAPTER TWO

INSTALLING CYBEREASON

Prerequisites

- Logpoint 7.2.0 or later
- Universal REST API Fetcher v2.2.0

To install Cybereason:

1. Download the .pak file from Help Center.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

CHAPTER

THREE

UNINSTALLING CYBEREASON

To uninstall Cybereason, you must delete all the log sources created using the Cybereason template.

To delete the Log Sources:

1. Go to *Settings >> Log Sources* from the navigation bar.
2. Click the (⋮) icon of log source and click **Delete**.

To uninstall Cybereason:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** (🗑) icon in **Actions** of Cybereason.

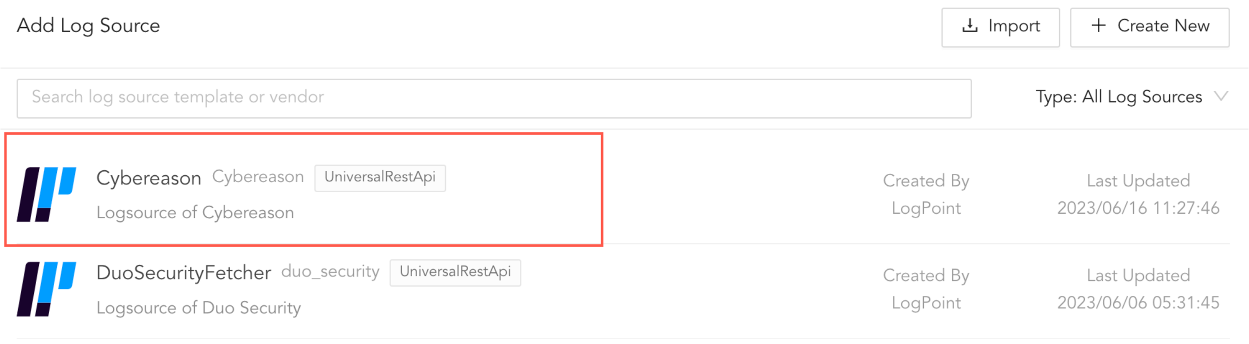
CHAPTER FOUR

CONFIGURING CYBEREASON

Cybereason consists of the log source template **Cybereason** which has predefined settings and configurations to fetch *Cybereason Malop* logs. However, there are some configurations that must be done manually.

To configure:

1. Go to *Settings >> Log Sources* from the navigation bar and click **Browse Log Source Templates**.
2. Click **Cybereason**.

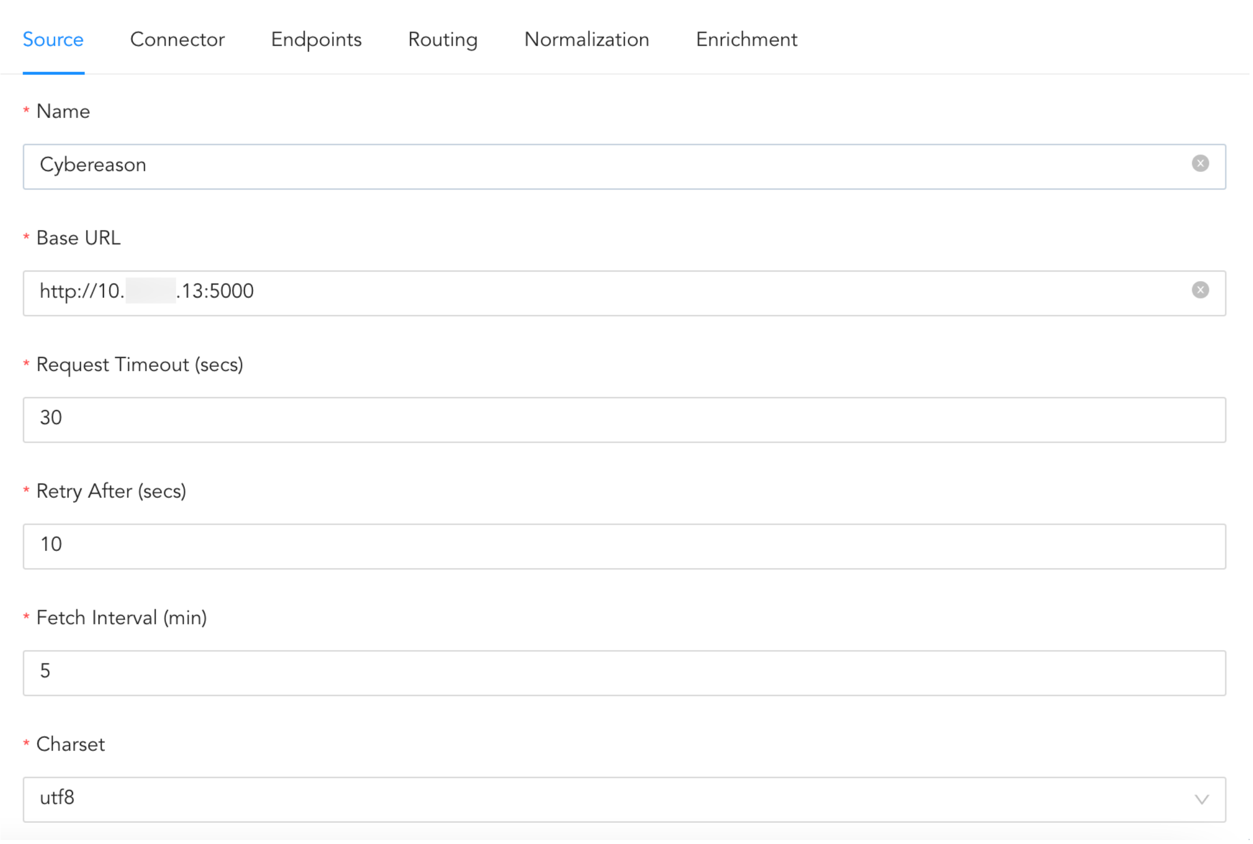


Cybereason Cybereason UniversalRestApi
Logsource of Cybereason
Created By LogPoint
Last Updated 2023/06/16 11:27:46

DuoSecurityFetcher duo_security UniversalRestApi
Logsource of Duo Security
Created By LogPoint
Last Updated 2023/06/06 05:31:45

Fig. 1: Log Source Templates

3. In **Base URL**, enter the endpoint URL and port number using the *https://<your server>:port number* format. For example, *http://1.1.1.1:50*.



* Name

Cybereason

* Base URL

http://10.[redacted].13:5000

* Request Timeout (secs)

30

* Retry After (secs)

10

* Fetch Interval (min)

5

* Charset

utf8

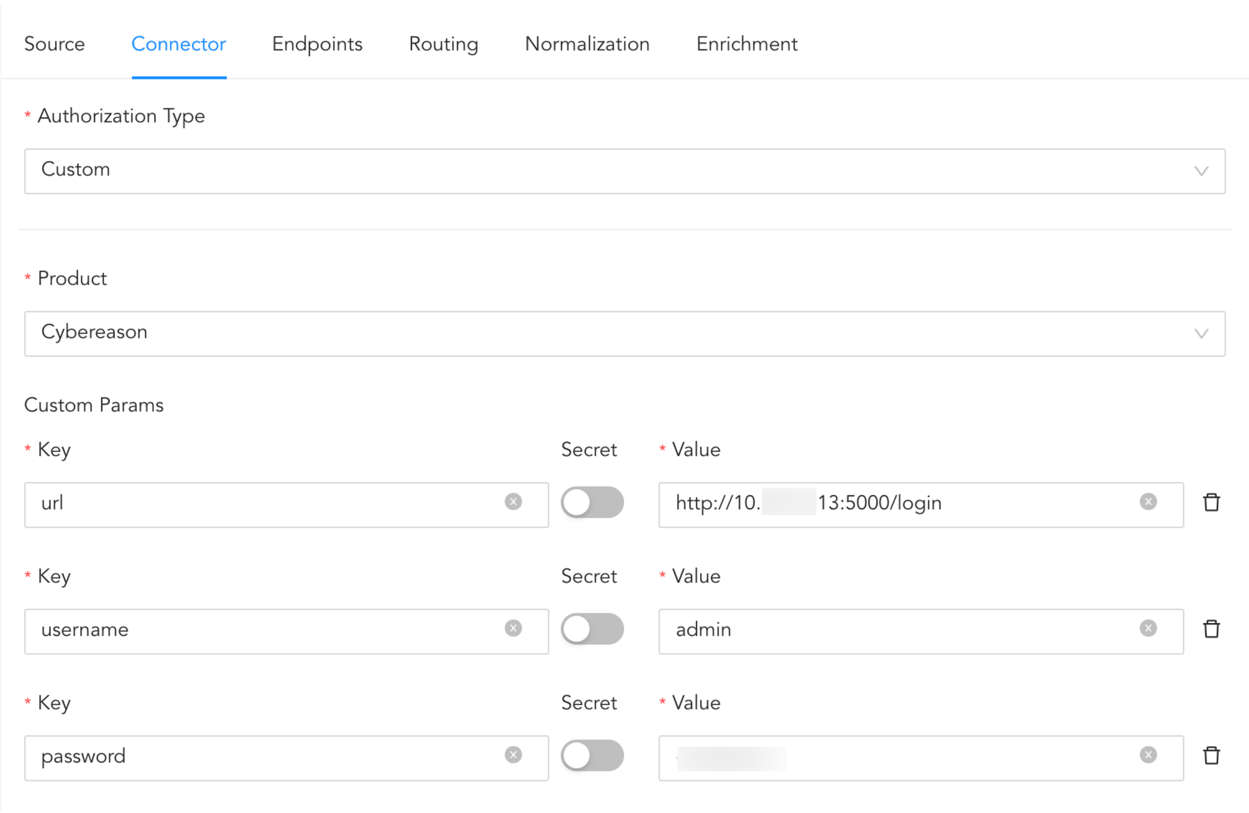
Fig. 2: Configuring Source

4. Click **Connector**.

5. In **Custom Params**,

   5.1. In *url* **Value**, enter the previously entered **Base URL** in the *https://<your server>:port number/login* format. For example, *http://1.1.1.1:50/login*.

   5.2. In *username* **Value**, enter your server's username and in *password* **Value**, enter your server's password.



* Authorization Type

Custom

* Product

Cybereason

Custom Params

* Key	Secret	* Value
url	○	http://10.[redacted]13:5000/login
username	○	admin
password	○	[redacted]

Fig. 3: Configuring Connector

6. Click **Routing** to create repos and routing criteria.

   6.1. Click **Routing** and **+ Create Repo**.

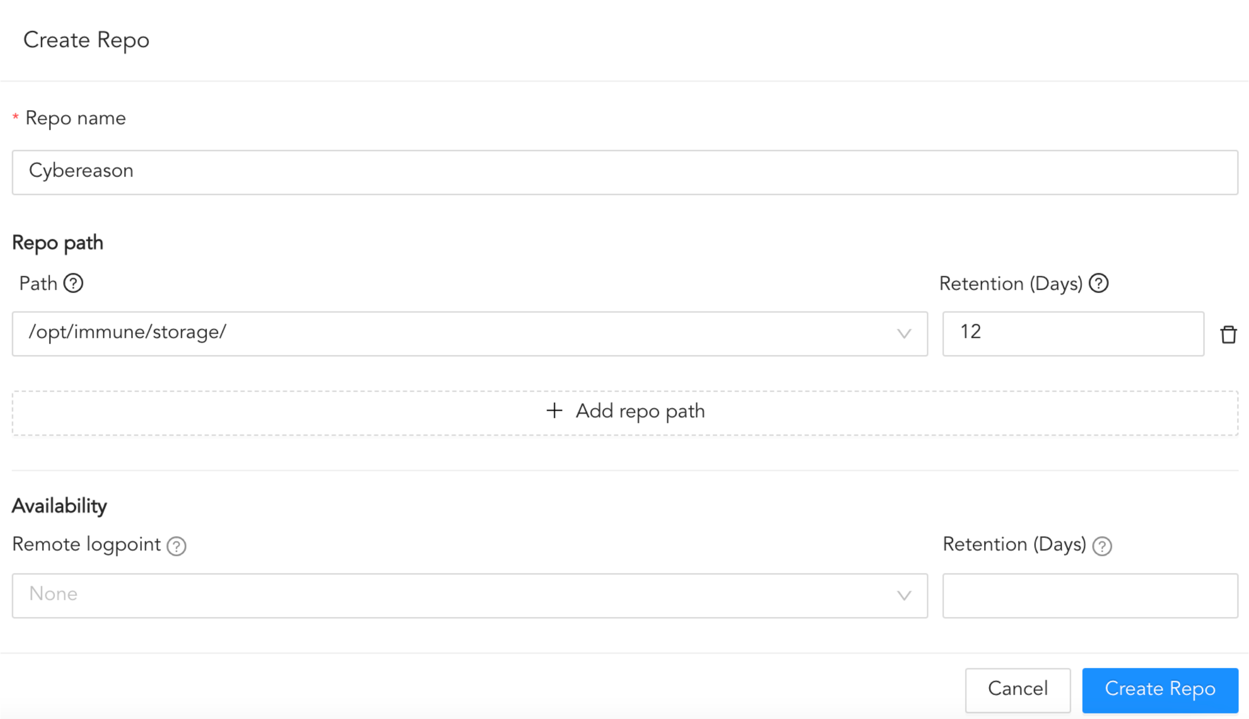
   6.2. Enter a **Repo name**.

   6.3. In **Path**, enter the location to store incoming logs.

   6.4. In **Retention (Days)**, enter the number of days logs are kept in a repository before they are automatically deleted.

   6.5. In **Availability**, select the **Remote logpoint** and **Retention (Days)**.

   6.6. Click **Create Repo**.



Create Repo

* Repo name

Cybereason

Repo path

Path: /opt/immune/storage/

Retention (Days): 12

Availability

Remote logpoint: None

Retention (Days):

Fig. 4: Creating a Repo

6.7. In **Repo**, select the created repo to store Cybereason logs.

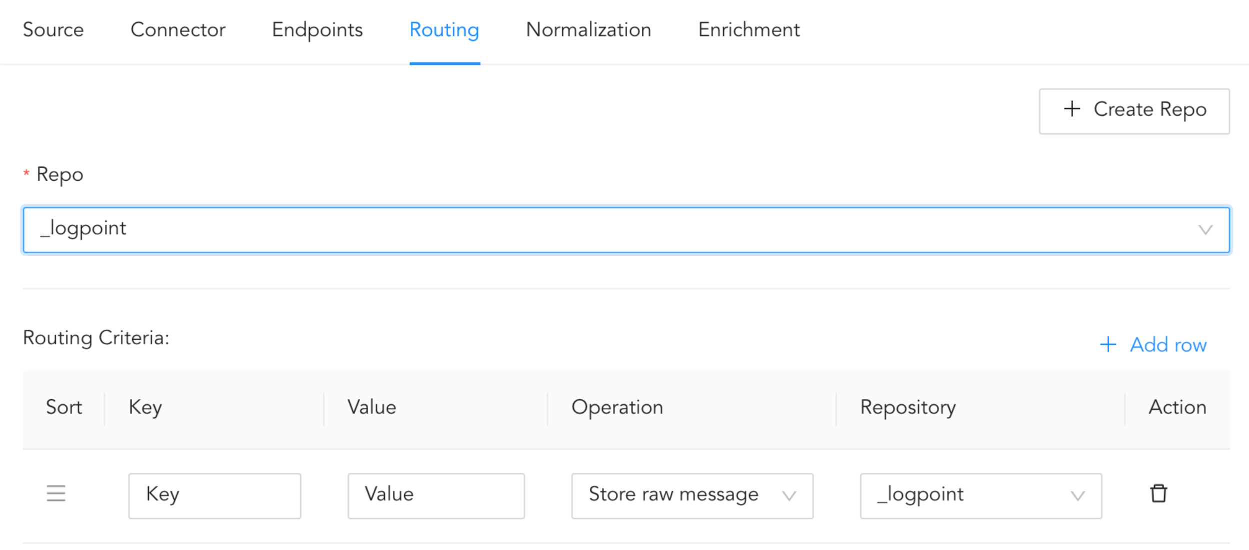
6.8. Click **+ Add row**.

6.9. Enter a **Key** and **Value**. The routing criteria are only applied to those logs which have this key value pair.

6.10. Select an **Operation** for logs that have this key value pair.

> 6.10.1. Select **Store raw message** to store both the incoming and the normalized logs in the selected repo.
>
> 6.10.2. Select **Discard raw message** to discard the incoming logs and store the normalized ones.
>
> 6.10.3. Select **Discard entire event** to discard both the incoming and the normalized logs.

6.11. In **Repository**, select a repo to store logs.



* Repo

_logpoint

Routing Criteria:

Sort	Key	Value	Operation	Repository	Action
☰	Key	Value	Store raw message	_logpoint	🗑

Fig. 5: Creating a Routing Criteria

Note: Click the (🗑) icon under **Action** to delete the created routing criteria.

7. Click **Enrichment** and select an enrichment policy for the incoming logs.
8. Click **Save Configuration** to save all the above configurations.

CHAPTER

FIVE

CYBEREASON ANALYTICS

5.1 Cybereason Search Template

The Cybereason search template provides dashboards consisting of predefined search queries with criteria and conditions to search for particular events and patterns in the incoming logs. There are two dashboards: Malops Overview and Malops Detection.

The Malops Overview dashboard provides a comprehensive view of detected malops, including information about the involved users, a timeline of malop events and the overall detection count.

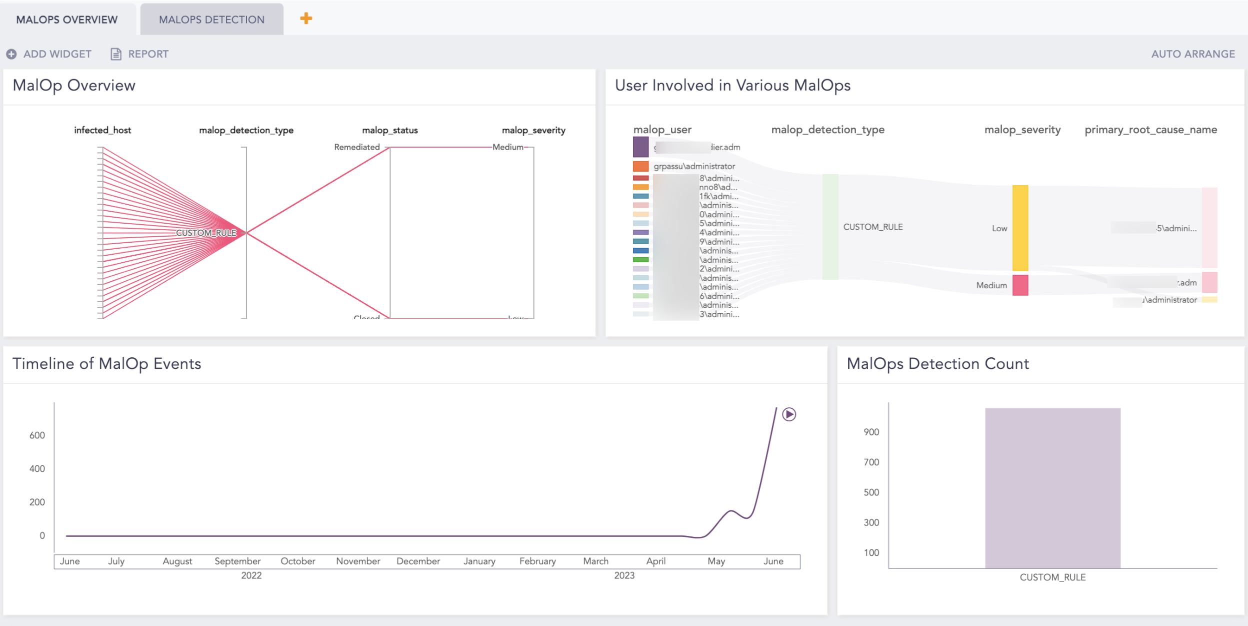


Fig. 1: Malops Overview

The Malops Detection dashboard provides in-depth insights into individual malops. It includes details such as a list of hosts with the highest malop detection, the primary root cause of the malop, administrative users with a significant number of malops and users who have experienced a high volume of malop events.

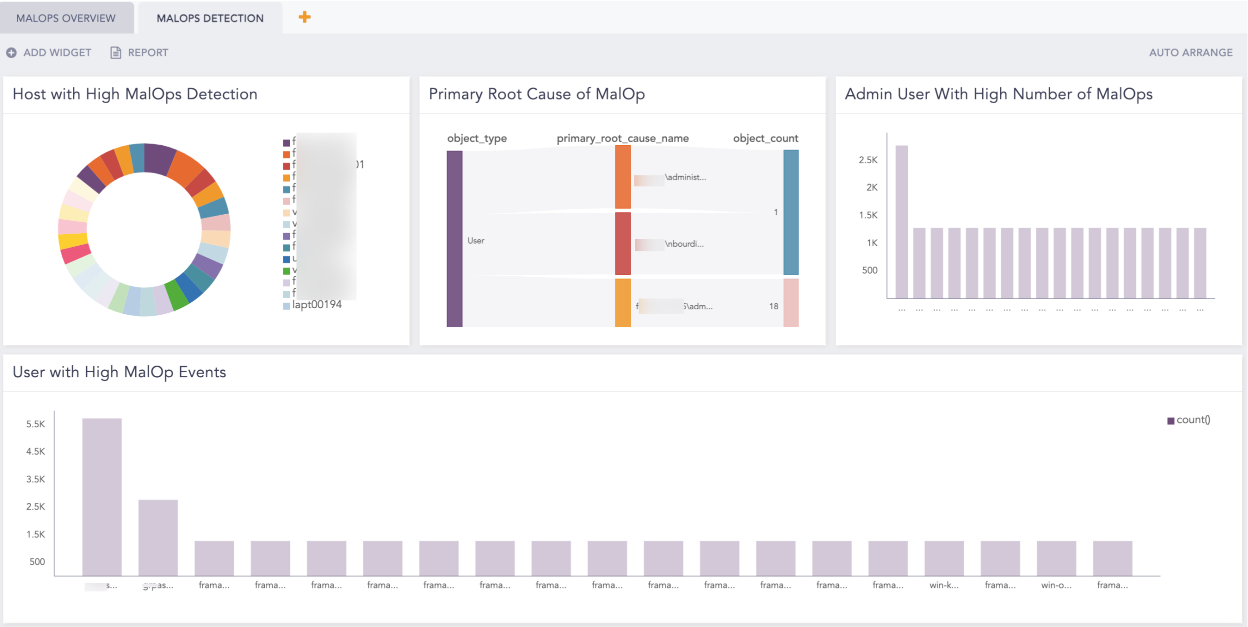
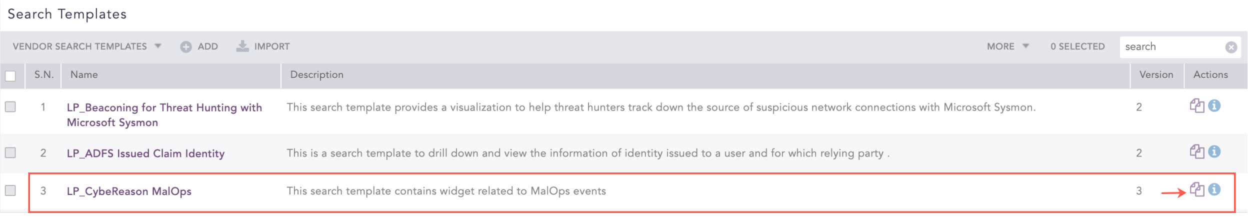


Fig. 2: Malops Detection

5.1.1 Viewing the Cybereason Search Template

1. Go to **Search Templates** from the navigation bar.
2. Select **VENDOR SEARCH TEMPLATES** from the drop-down.
3. Click the clone icon from **Actions**.

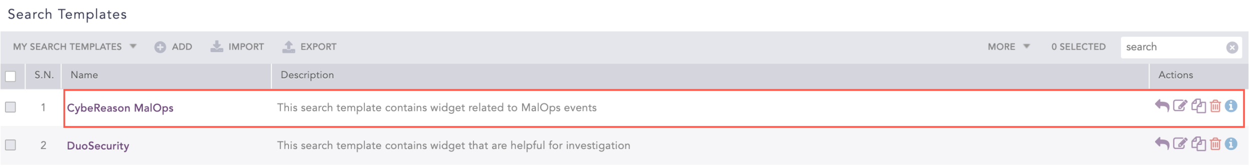


□	S.N.	Name	Description	Version	Actions
□	1	LP_Beaconing for Threat Hunting with Microsoft Sysmon	This search template provides a visualization to help threat hunters track down the source of suspicious network connections with Microsoft Sysmon.	2	
□	2	LP_ADFS Issued Claim Identity	This is a search template to drill down and view the information of identity issued to a user and for which relying party .	2	
□	3	LP_CybeReason MalOps	This search template contains widget related to MalOps events	3	

Fig. 3: Cloning Cybereason Search Template

Logpoint forwards you to **MY SEARCH TEMPLATE**.

4. Click **CybeReason MalOps**.



S.N.	Name	Description	Actions
1	CybeReason MalOps	This search template contains widget related to MalOps events	
2	DuoSecurity	This search template contains widget that are helpful for investigation	

Fig. 4: Cybereason Search Template

Logpoint forwards you to **Search Template View**.

3. Click **Update** to access the dashboards of the search template.

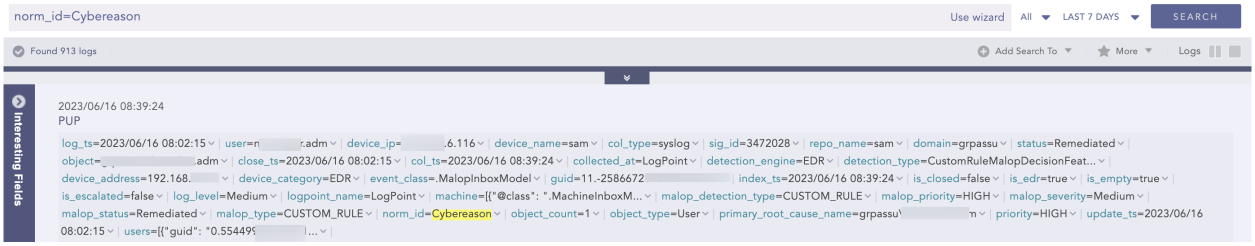
CHAPTER

SIX

ACCESSING CYBEREASON LOGS

Use the following query to access the logs:

```
norm_id=Cybereason
```



```
norm_id=Cybereason
Found 913 logs

2023/06/16 08:39:24
PUP
log_ts=2023/06/16 08:02:15 | user=n[redacted]r.adm | device_ip=[redacted].6.116 | device_name=sam | col_type=syslog | sig_id=3472028 | repo_name=sam | domain=grpassu | status=Remediated |
object=[redacted].adm | close_ts=2023/06/16 08:02:15 | col_ts=2023/06/16 08:39:24 | collected_at=LogPoint | detection_engine=EDR | detection_type=CustomRuleMalopDecisionFeat... |
device_address=192.168.[redacted] | device_category=EDR | event_class=.MalopInboxModel | guid=11.-2586672[redacted] | index_ts=2023/06/16 08:39:24 | is_closed=false | is_edr=true | is_empty=true |
is_escalated=false | log_level=Medium | logpoint_name=LogPoint | machine=[{"@class": ".MachineInboxM... | malop_detection_type=CUSTOM_RULE | malop_priority=HIGH | malop_severity=Medium |
malop_status=Remediated | malop_type=CUSTOM_RULE | norm_id=Cybereason | object_count=1 | object_type=User | primary_root_cause_name=grpassu\[redacted]m | priority=HIGH | update_ts=2023/06/16
08:02:15 | users=[{"guid": "0.55449[redacted]l... |
```

Fig. 1: Cybereason Log