CYBER 2.0

LOG READER V5

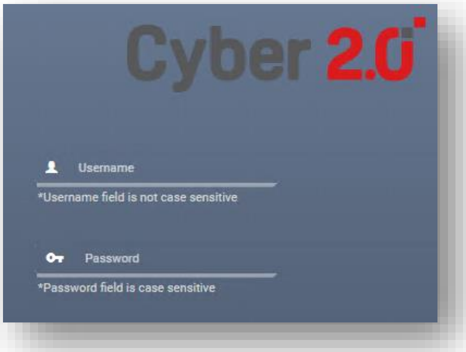
Description

This is an updated and approved version of the log reader tool. This tool is a network monitoring tool.

The logs are displayed in chronological order by server time.

Features

- Active applications on network logs
- File system access logs
- Broadcast monitoring
- Chains of every process
- Status of approved and unapproved programs



Cyber 2.0

Username

*Username field is not case sensitive

Password

*Password field is case sensitive

Accessing

In order to access the V5 log reader interface ,

you should enter the following address:

http://{cyber 2.0 server IP}:9000

Username: superuser

Password : Cyber@123

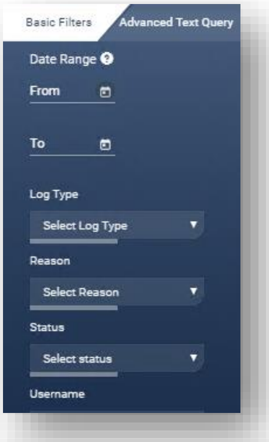
Capabilities

Filtering – on the left side of the screen there are basic filter options.

To apply them , choose the desired filter then press enter or

click on the checkmark above the table : ✓

There are more filter options available than seen in the picture



Basic Filters | Advanced Text Query

Date Range

From

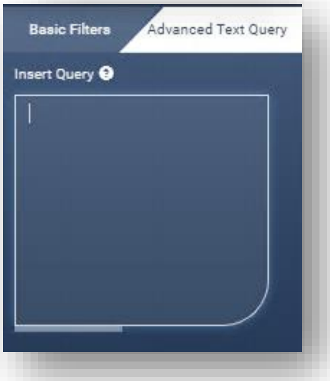
To

Log Type: Select Log Type

Reason: Select Reason

Status: Select status

Username



Basic Filters | Advanced Text Query

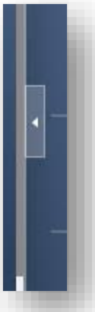
Insert Query

Advanced filtering – next to the basic filters there's an “advanced text query” tab The text box that appears allows you to enter wanted filters and use the “+” sign to add more wanted filters. Representation

: And = + , Or = | , Not = - . Query for example: vlc.exe + - ok +|blocked

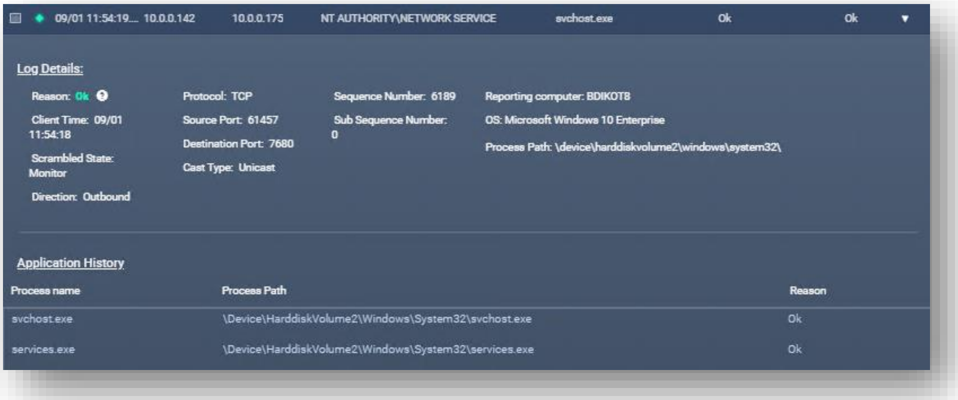
This query means that I want to get all the logs for vlc.exe and that status is not ok or blocked. To apply the filter press enter.

- If you wish to hide the filters section there is an arrow on the side.



Log information

When selecting a row , it expands and shows you more details about that certain log.



□ 09/01 11:54:19... 10.0.0.142 10.0.0.175 NT AUTHORITY\NETWORK SERVICE svchost.exe Ok Ok ▼

Log Details:

Reason: Ok

Client Time: 09/01 11:54:18

Scrambled State: Monitor

Direction: Outbound

Protocol: TCP

Source Port: 61457

Destination Port: 7680

Cast Type: Unicast

Sequence Number: 6189

Sub Sequence Number: 0

Reporting computer: BDIKOT8

OS: Microsoft Windows 10 Enterprise

Process Path: \device\harddiskvolume2\windows\system32\

Application History

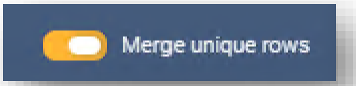
Process name	Process Path	Reason
svchost.exe	\Device\HarddiskVolume2\Windows\System32\svchost.exe	Ok
services.exe	\Device\HarddiskVolume2\Windows\System32\services.exe	Ok

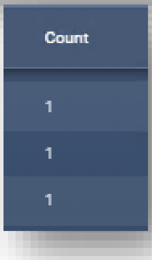
Reporter view

To change to reporter view you need to select the “merge unique rows” toggle.

This will merge all the logs with the same data and will add counter to display the amount of times this activity has occurred.

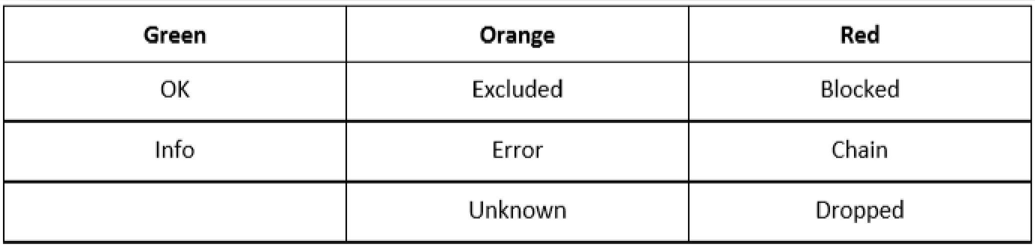
By using this the user can notice unusual activity in the system, rows with count 1 can be suspicious and rows with a very high counter can describe a legitimate activity or an alert for bruteforce attempts.





Count
1
1
1

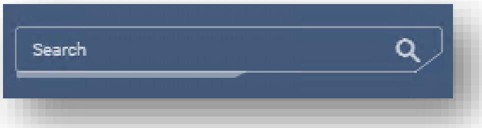
Next to each log there is a notification color , the colors represent the statuses :



Green	Orange	Red
OK	Excluded	Blocked
Info	Error	Chain
	Unknown	Dropped

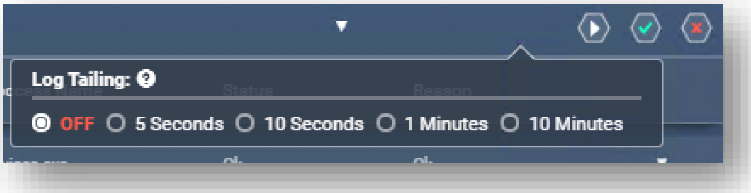
Free search

The free text search enables to search any data that the logs contain (viewed data / hidden data in the expandable row). The user can search for any data that the table contains. Fields: source IP, destination IP, process path, username, process name, status, reason, protocol, directions, ports, OS, cast type, scramble state, policy, reporting computer, DLL name, destination path, process ID.



Log tailing

The log tailing feature refreshes the view automatically at a selected time, this provides the user full tracking over the logs.

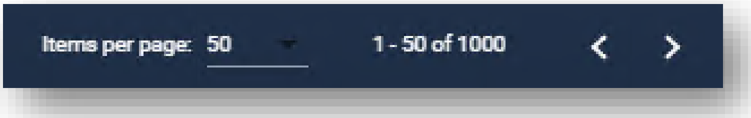


Log Tailing:

● OFF ○ 5 Seconds ○ 10 Seconds ○ 1 Minutes ○ 10 Minutes

Paging

The user can page the table to view more logs or change the rows that are displayed per page.



Items per page: 50

1 - 50 of 1000