



Day 4

ZROC102

Module 2: Log Management



LETSDEFEND Platform

≡ LogManagement

Freemium ▾




- Homepage
- Tutorial >
- Training new
- Monitoring
- Log Management**
- Case Management
- Endpoint Security
- Mailbox

Log Search

Result: 7 ▾ Page: 1 ▾

Search...

Search

#	↑↓ DATE	↑↓ TYPE	↑↓ SOURCE ADDRESS	↑↓ SOURCE PORT	↑↓ DESTINATION ADDRESS	↑↓ DESTINATION PORT	↑↓ RAW
1	Aug, 29, 2020, 07:28 PM	Proxy	172.16.17.14	47741	198.100.45.154	80	
2	Aug, 29, 2020, 07:32 PM	Proxy	172.16.17.14	57441	67.68.210.95	80	
3	Aug, 29, 2020, 08:00 PM	Exchange	63.35.133.186	47847	172.16.20.3	25	

Log Management

This is the Log Management Section that houses all logs of all devices in this simulation, to be viewed and analyzed. The search bar can be used to perform general searches.

LogManagement

Freemium

Log Search

Result: 7 Page: 1

Search... Search

#	DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
1	Aug, 29, 2020, 07:28 PM	Proxy	172.16.17.14	47741	198.100.45.154	80	
2	Aug, 29, 2020, 07:32 PM	Proxy	172.16.17.14	57441	67.68.210.95	80	
3	Aug, 29, 2020, 08:00 PM	Exchange	63.35.133.186	47847	172.16.20.3	25	
4	Aug, 29, 2020, 08:09 PM	Proxy	172.16.17.88	23477	81.169.145.105	80	
5	Sep, 18, 2020, 02:14 PM	Firewall	172.16.17.35	4421	173.231.198.30	587	
6	Sep, 20, 2020, 07:54 PM	Firewall	172.16.17.47	54211	5.188.0.251	443	
7	Sep, 20, 2020, 07:54 PM	Proxy	172.16.17.47	54211	5.188.0.251	443	

Search

Search Date

Search Type

Search Src Address

Search Src Port




Search Dst Address

Search Dst Port

Clear

Log Management

There are searches under the columns for specific searches.

5	Sep, 18, 2020, 02:14 PM	Firewall	172.16.17.35	4421	173.231.198.30	587	
6	Sep, 20, 2020, 07:54 PM	Firewall	172.16.17.47	54211	5.188.0.251	443	
7	Sep, 20, 2020, 07:54 PM	Proxy	172.16.17.47	54211	5.188.0.251	443	
<div><div>Search</div><div>Search Date</div><div>Search Type</div><div>Search Src Address</div><div>Search Src Port</div><div>Search Dst Address</div><div>Search Dst Port</div><div>Clear</div></div>							

Log Management

Example: Searching for a url “**google.com**”, notice we have five(5) entries displayed.

Log Search

Result: 7

Page: 1

google.com

Search

#	DATE	TYPE	SOURCE ADDRESS	SOURCE PORT	DESTINATION ADDRESS	DESTINATION PORT	RAW
9	Oct, 11, 2020, 06:39 PM	Proxy	172.16.17.47	23312	172.217.17.238	443	+
10	Oct, 11, 2020, 06:41 PM	Proxy	172.16.17.47	41221	172.217.17.238	443	+
18	Oct, 19, 2020, 07:59 PM	Proxy	10.15.15.12	14774	172.217.169.206	443	+
319	Dec, 20, 2020, 02:10 PM	Proxy	172.16.17.55	49283	172.217.17.174	443	+
320	Dec, 20, 2020, 02:11 PM	Proxy	172.16.17.55	47283	172.217.17.174	443	+

Search

Search Date

Search Type

Search Src Addr

Search Src Port

Search Dst Address

Search Dst Port

Clear

Log Management

Example: To narrow down our search, searching for the url “**google.com**”; we can also search for a specific Source IP Address. Notice two(2) entries are displayed.

Log Search

Result:

7 ▾

Page:

1 ▾

google.com

1

Search

#	↑↓ DATE	↑↓ TYPE	↑↓ SOURCE ADDRESS	↑↓ SOURCE PORT	↑↓ DESTINATION ADDRESS	↑↓ DESTINATION PORT	↑↓ RAW
9	Oct, 11, 2020, 06:39 PM	Proxy	172.16.17.47	23312	172.217.17.238	443	
10	Oct, 11, 2020, 06:41 PM	Proxy	172.16.17.47	41221	172.217.17.238	443	

Search

Search Date

Search Type

172.16.17.47

2

Search Src Port

Search Dst Address

Search Dst Port

Clear

Source

- <https://app.letsdefend.io/logmanagement/logs/>
- <https://app.letsdefend.io/tutorial/videos/>