

How to – Configure Malwarebytes Nebula (cloud) to forward logs to EventTracker

EventTracker v9.2 and later

Abstract

This guide provides instructions to retrieve the **Malwarebytes Nebula** events via syslog. Once the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Malwarebytes Nebula (cloud platform)**.

Audience

Administrators who are assigned the task to monitor **Malwarebytes Nebula** events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview	3
2. Prerequisites	3
3. Integrating Malwarebytes Nebula with EventTracker	3
3.1 Configuring Malwarebytes Nebula to forward logs to EventTracker	3

1. Overview

Malwarebytes Nebula is a cloud-based security platform for complete endpoint protection. It allows the user to manage products such as Malwarebytes Endpoint Protection, Malwarebytes Incident Response, Malwarebytes Endpoint Detection and Response from a single cloud-based user interface (UI).

EventTracker, when integrated with Malwarebytes Nebula, collects logs and creates detailed reports, alerts, dashboards, and saved searches. These attributes of EventTracker helps the user to view/receive critical and relevant information regarding security, operations and compliance.

Reports contain a detailed summary of security events such as malware detection, URL filtering, suspicious activity, potentially unwanted programs activities and modifications, and many more in column-value pair.

Alerts are triggered as soon as a critical event is received by EventTracker for Malwarebytes Nebula, such as malware detection, URL filtering, suspicious activity, potentially unwanted programs activities and modifications, etc.

Dashboards represent all the activities happening in Malwarebytes Nebula. These include event categories with cumulative log counts/percentage, events that are either blocked, quarantined, found, restored, or deleted, and timeline of occurrences of security related activities.

These attributes or configurations of EventTracker allows administrators to quickly take appropriate actions against any threat/adversaries trying to jeopardize an organization's normal operation.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Malwarebytes Nebula Web UI.
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager public IP address.

3. Integrating Malwarebytes Nebula with EventTracker

3.1 Configuring Malwarebytes Nebula to forward logs to EventTracker

1. Login into your Malwarebytes Nebula Web UI using admin credentials.

2. Go to **Settings > Syslog Logging**.
3. Click **Add**. Promote one of your windows endpoints as the syslog communication endpoints.

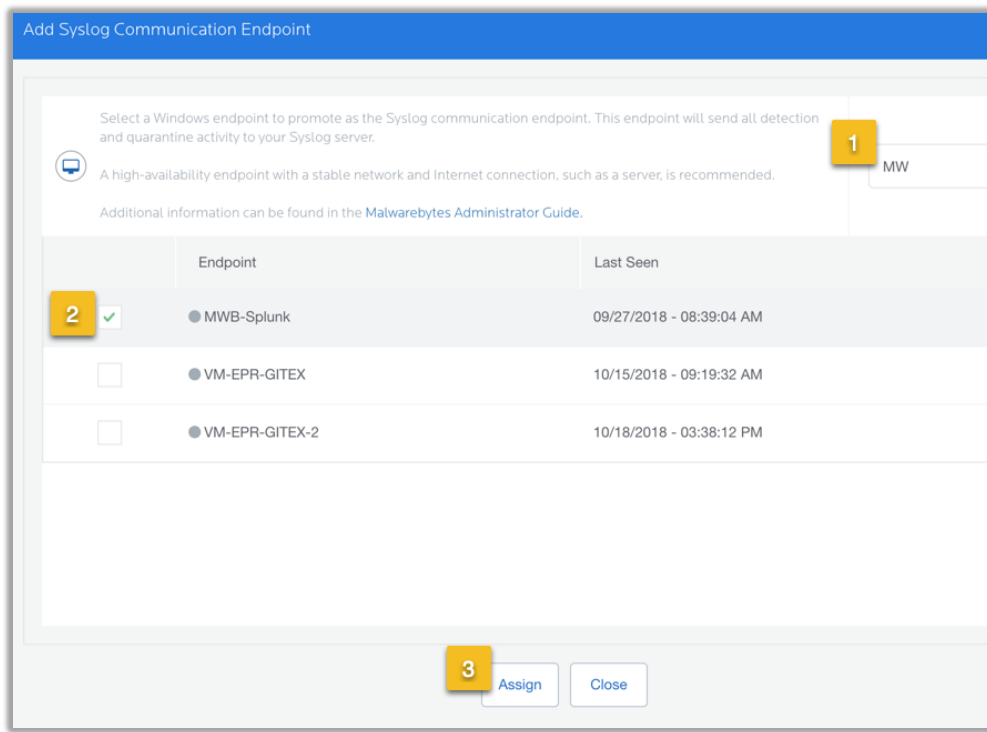


Figure 1

4. In the top-right corner, click **syslog settings**.
5. Fill in the following information, then click **Save**.
 - **IP Address/Host:** Public IP or hostname of your EventTracker manager.
 - **Port:** Port you have specified on your EventTracker manager. (e.g. 514)
 - **Protocol:** Select UDP protocol.
 - **Severity:** Choose a severity from the list. This determines the severity of all Malwarebytes events sent to syslog.
 - **Communication Interval (Minutes):** Determines how often the communication endpoint gathers syslog data from the Malwarebytes server. If the endpoint is unable to contact Malwarebytes, it buffers data from the last 24 hours. Data older than 24 hours is not sent to syslog.

Syslog Communication Settings

Specify your Syslog server settings below.

IP Address/Host:

Port (1-65535):

Protocol: TCP UDP

Severity (0-10):

Log Format: CEF

COMMUNICATION INTERVAL

Minutes (5-1440):

Figure 2

6. Navigate to **Endpoints**. Click on the syslog communication endpoint you assigned in Step 2.
7. In the **Agent Information** section, the SIEM version number displays. This confirms the SIEM plugin has activated on the endpoint.

malwarebytes Endpoints

Endpoint Properties:
Last Seen: 2019-11-01 12:05:41 PM

Overview

Agent Information

SIEM:	1.2.0.107
Operating System	

Figure 3

8. This confirms the syslog configuration of Malwarebytes Nebula.