Netsurion™ | EventTracker

Feature List

EventTracker v9.0

Publication Date: December 11, 2017

Abstract

This document gives a brief overview regarding the features that are newly introduced in EventTracker Enterprise version 9.0.

Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v9.0 version.

Table of Contents

Abstract 1
Audience 1
Major improvements in v9.0 3
Minor improvements in v9.0 4
New Knowledge Packs 5

Major improvements in v9.0

- **Redesign User Interface Themes with Improved experience**

  EventTracker v9.0 has a complete revamped User Interface, with added features and enhancements, making it more user-friendly and device-friendly. It will now have a changed color theme and layout with most of the standard features getting replaced. The Responsive and adaptive design helps the UI adjusts automatically to the device/resolution the user(s) uses.

- **EventTracker Common Indexing Model (CIM) introduced**

  All the logs/events are now normalized and mapped to common schema for the last 7 days.

  For Example: Just search with "**tags:"login failed"**" to get login failure results from any source (VPN, Active Directory, Firewall etc.) without worrying about event id or any other property.

- **Improved search performance with Elasticsearch**

  Elasticsearch is a search engine based on Lucene. It is distributed, multitenant-capable full-text search engine. It is used to store all events represented in EventTracker CIM for last 7 days.

- **Tear Away enhancement**

  The user now has as option to create their own page where they can add dashlets which keeps on displaying them in a new window and will refresh every selected (20 secs/1min/2 min...) interval.

- **Saved searches in widget configuration**

  The user can now use the pre-defined Saved searches for configuring Widgets and adding them to the Dashboard.

- **Exposed tabular data as a new dashlet type**

  For Dashlet configuration, the chart type "Tabular" has been added. Selecting Tabular will display the respective data in tabular format.

- **Export/Import of dashlets in Compliance Dashboard**

  Now, for compliance dashboard, dashlets can be exported as well as imported as per requirement.

- **Creating dashlets from Log Search**

  The log search result can now be created as dashlets and added to dashboards.

- **Enable/Disable option for sub-folder monitoring**

  An option for sub-folder monitoring is provided to add filter for each sub-folder which helps in avoiding the noise event.

- **Specific registry/folder monitoring can be enabled/disabled at system as well as global level**

  In EventTracker 9.0, the specific registry monitoring can be enabled/disabled both at the system level and global level.

- **Controlling the size of flex dashlets**

  The configured dashlets can be re-sized as per requirement.

- **Admin Diagnostics redesigned dashboard is available**

Minor improvements in v9.0

- Enhancement in application and network connection monitoring for identification of new hash and unique IP address in the network.

- Support for VMware vCenter 6.0 and later: Support for reading logs from vSphere 6.5 in Agent LFM.

- Change Audit: Default configuration is now based on windows file/registry auditing best practices.

- No device specific Knowledge Objects are imported automatically during setup. All relevant KOs need to be imported during initial setup. All Knowledge Objects are distributed in the setup and available in new folder structure under "**EventTracker->Knowledge Packs**".

- Renamed the "**Logbook**" feature to "**Casebook**".

- "**Event Category**" is now known as "**System defined - Saved Search** "in EventTracker v9.0.

- EventTracker Console/Manager can only be installed on 64-bit windows.

- Windows sensor is no longer supported on Windows XP and Windows Server 2003. The Minimum supported operating systems are Windows Vista and Windows Server 2008.

New Knowledge Packs

- **Duo Security**
- **Akamai Web Application Firewall**
- **Carbon Black**
- **Tenable.io**
- **Microsoft Antimalware**
- **Carbon Black Protection**
- **Check Point Firewall**
- **Cisco IOS**
- **ET VAS**
- **HAProxy Server**
- **VMWare**
- **Webroot Antivirus**
- **Websense Security Gateway (WSG)**
- **Windows Storport**
- **FileZilla**
- **Bitvise SSH**
- **WarFTP**
- **Mimecast**
- **Sophos XG Firewall**
- **Pulse Secure**
- **Vectra Threat Detection**