EventTracker
Secure. Comply. Succeed.

Feature List

EventTracker v8.1

Publication Date: Jan. 28, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This document gives a brief overview regarding the features that are newly introduced in EventTracker Enterprise version 8.1.

Target Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v8.1 version.

Table of Contents

Major improvements in v8.1

- **Unknown Processes Dashboard**

  In EventTracker v8.1, a new dashboard named **'Unknown Processes'** is designed to interpret advanced threats and false positives which emerge within an enterprise. Whenever a new process is launched in a machine, it will look up for emerging threats, if any. The user will be able to filter the unknown processes based on Signature status. Also the user will be able to filter the unknown processes that are not digitally signed for which he might be interested. He can also add the unknown processes to Safe/Unsafe list as per requirement.

- **Attackers Dashboard**

  - EventTracker now uses the service providers: IP Void and IBM XFE to locate the Blacklisted IPs and for displaying the geo location; it uses the providers: MaxMind Geolite and IP Void.

  - Attackers dashboard will now have an option to add various threat intelligence platforms, e.g. Autoshun, BorderWare, Dshield, etc. This will be useful for a user to investigate the evilness of an IP address.

- **Reports**: Display Excel report in HTML format with sort and filter options.

- **Dashboard>Threats**: The Attackers dashboard has been renamed as Threats.

- **Parsing Rule**: Search option has been provided in Parsing Rules>Token Templates. The user can now search the templates by name.

- **DLA**: DLA now includes JSON and ETL format log files.

- **Alert Management**: In Admin>Alerts, while configuring an alert action, under e-mail configuration, the **Alert Footer** and **Alert e-mail subject prefix fields** are added.

- CP-CM: Considering SQL Server for CP cab details instead of MS Access database.

- **Flex Dashboard:** Provide range and color selection for meter gauge.

- **New Benchmarks** added:
  - Microsoft Office Lync 2013
  - Windows 8 and 8.1
  - Windows 2012 R2

Minor improvements

- **User config**: Provide option to search by user for user config and logo customization module.
- **Report**: Add new options to set schedule for Daily and Weekly report.
- **Systems**: Some new default system groups has been added in Admin>Systems.

Others

- **Index Explorer**: The Index Explorer option has been removed from the **Tools** menu.
- **Change Audit**: In Change Audit>System Inventory, the tabs '**Application Installed"** and '**Updates"** has been removed.

❖ **Updated Categories**

- Windows Audit Log Clear

❖ **Updated Alerts**

- Cyberoam UTM: Attack Detected
- Cyberoam UTM: Spam Detected
- Cyberoam UTM: Virus Detected
- FortiGate: Administrator Logon Failed

❖ **Updated Flex Reports**

- Clavister-User Authentication Failed
- MySQL-Authentication Failed
- MySQL-Authentication Success
- MySQL-Database Management
- MySQL-Database Query Log Detail

- MySQL-Privileges Change
- MySQL-Table Management
- Windows-Application Crash Analysis
- Windows-User Account Locked
- EventTracker-Bad IP Reputation network activity