Netsurion™ | EventTracker

Feature List

EventTracker v8.3

Publication Date: May 26, 2017

Abstract

This document gives a brief overview regarding the features that are newly introduced in EventTracker Enterprise version 8.3.

Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v8.3 version.

Table of Contents

Major improvements in v8.3

- **Enhancement in LFM to consider the date and time mentioned in the log file.**

The earlier Agent LFM configuration always considered current system date and time after parsing the records. To overcome this, we have now provided standard and custom date and time formats to configure Agent LFM. Now the configured files in the Agent LFM will be parsed as per the selected date and time formats.

- **Agent health check enhancements.**

As per the enhancement, a new service named "**EventTracker Monitoring Daemon**" gets added. It monitors the EventTracker agent activities including Memory, Handles, CPU Time, and Counter Check (evtViewerLog.etw).

- **Enhancement in Direct Log Archiver (DLA) to specify different Virtual Collection Point (VCP) for each configuration.**

The user can now configure a DLA configuration by using different VCP port selection and the log parser now picks all the configurations to parse at the same time as per the port selected.

- **Enhancement in User Management.**

The MSP feature provided will serve the sole purpose of managing subscription related activities such as managing user accounts and monthly usage details of services provided by EventTracker per client.

This enhancement in User Management provides a new feature "**Managed Service Provider (MSP) in User management**", while enabling Database Authentication.

- **Option to configure Active Watch List lookup in Alert Configuration**

This option allows the user(s) to configure alerts by extracting the values from the event and compare it against the Active Watch List. If the admin maintains a local black/white list data, he/she can configure the alerts and compare it with Active Watch list, based on which the alert will be triggered.

- **STIX/TAXII support in EventTracker.**

This feature connects to any of the TAXII Server(s) to collect the Feeds such as IP, Domain, URL, etc. to EventTracker.

- **Ability to forward syslog messages through EventTracker agent**

The raw syslog messages are received by EventTracker agent on configured syslog port. EventTracker agent encrypts the messages and forward to EventTracker cloud server over internet.

- **Handle user permission in attackers and targets dashboard**

This helps in handling group level permission in Attacks & Targets Dashboard.

- **Support for Identifying unknown/unsafe dormant executable files in the network.**

- **Customizable alert email content based on HTML templates.**

- **EventVault explorer, Behavior and Tile Dashboard enhancement**

EventVault Explorer

With the new User Interface enhancement provided, the EventVault Explorer now supports the following changes:

- Faster Data loading.
- Quick access to columns with the top records.
- Time Selection options (Quick, Relative and Absolute).
- Expand and Collapse for the available column option.
- Include/Exclude metadata from available columns.

Tiles Dashboard

The Tiles Flip happens if total incident count is equal to the acknowledged count, informing that this tile is of least importance. Tile Flip for those tile(s) makes the process hassle-free so that other incidents get noticed.

Minor improvements in v8.3

- An Enhancement in Network Monitoring to monitor listening ports.
- Configure an alert only for systems with given asset value under a given system group.
- Option to configure "Set As Start Page" in EventTracker Enterprise.
- amCharts for better data visualization in Flex dashboard, Incidents and Behavior Dashboard.
- The map control has been replaced from Google Maps to amMaps in Attackers dashboard & Behavior dashboard.
- Direct Log Archiver: Option to configure number of files to be processed in a cycle.
- Multiple Selection of Reports (**Maximum: 5**) and download the Reports as zip file, from the Report Dashboard.
- To avoid scrolling, an option (Back to Top/Go to bottom) has been provided, which allows the user to navigate between Top/Bottom page and its details in Event Tracker application.

- The Top Level Summary report now has Real Time and File Transfer columns for Event count and Computer count.

Updated KP Items

❖ **Updated Alerts**

- Cisco IronPort ESA: Email bounced
- Cisco IronPort ESA: User authentication failed
- Cisco IronPort WSA: Web access blocked
- Cisco Sourcefire: High priority alert generated
- Juniper Netscreen: IP address conflict
- Juniper Netscreen: VPN service down

❖ **Updated Flex Reports**

- Windows Audit Log Cleared Report
- Windows User Logon or Logoff Success Report
- Windows Active Directory Object Access Report
- Windows Software Install or Uninstall on System Report
- Microsoft DNS-Name resolution failure
- Microsoft DNS-Name resolution success
- BIG-IP LTM-System configuration changed
- Cisco IronPort WSA-Web access allowed
- Cisco IronPort WSA-Web access denied
- Cisco ASA-IDS intrusion detection
- Cisco ASA-Connection denied

❖ **Updated Categories**

- Cisco IronPort ESA: Email bounced
- Cisco IronPort ESA: User authentication failed
- Cisco IronPort ESA: User authentication success
- Cisco IronPort WSA: Web access allowed
- Cisco IronPort WSA: Web access blocked