EventTracker

Actionable Security Intelligence

Feature List

EventTracker v8.2

Publication Date: June 10, 2016

Abstract

This document gives a brief overview regarding the features that are newly introduced in EventTracker Enterprise version 8.2.

Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v8.2 version.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

Table of Contents

Major Improvements

Tile Dashboard

To make the Incidents feature more interactive, EventTracker now introduces a new dashboard named Tile Dashboard (**Incidents -> Tile View**). This dashboard will help the user in getting the minute information related to the alert in a more precise way.

This new feature is provided to view the “Alert detail” in a tile format. This will show the number of “Incidents” generated for that “Alert”, last occurred time of an incident, severity and number of actions taken for that alert, acknowledged/unacknowledged/Flagged and number of annotated count.

Log Search as a Task

EventTracker now initiates that the log search process runs in the background. When a user performs a search, a notification will be displayed at the bottom of the page, which will indicate that the search is launched. When the search task will be having results to display, a small pop-up window gets displayed. The user can click the task window and view the search results in a new window.

CP generated reports to be seen in CM

Collection Master will now have the ability to show the Collection Point reports and Top Level Summary reports.

- User can see the generated reports and TLS reports for CP.
- User can Add to logbook.
- User can see the Report configuration and exceptions.
- User can Add notes for CP reports.
- User can change the Flag status for CP reports.

Configure Archive path for each VCPs

The EventVault configuration window will now have a list view, which will display the configured ports and their respective configured archive path.

The Ports configured by the user in Manager>Syslog/Virtual Collection Point, will now be listed in EventVault configuration window and the user can configure archive path for specific VCPs.

Event Filter Enhancement

EventTracker now adds the option to configure filters for Global, Archiver and Receiver in **Admin -> Event Filters**.

- All the configured filter events will now be dropped, which in turn will minimize the archive database storage.
- The user can now filter both real time and offline events using the filter types:
  - **Global**
  - **Archive**
- The feature will also filter out the real time events after alerting has been performed **(Selecting Archive** as **Filter type).**
- The user will also be able to configure a filter by selecting specific systems/ groups and also specific VCP ports.

Agent Filter Enhancement

EventTracker now provides **OR** and **&&** operators in EventTracker Agent configuration as well as in EventTracker Web for Match in User and in Match in Source.

Agent Version Request

A new option "Query for agent version info "has been included in "Admin -> System Manager" and "EventTracker Control Panel -> Agent Management Tool". The option will query for the agent version info and the report generated will display sufficient details of files and updates related to the remote agent.

Knowledge Object Grouping

User can now categorize the knowledge objects by creating customized groups and adding Knowledge Objects to the group, as per requirement.

- Search Knowledge Objects
- Add/Edit Group
- Add Objects to Group
- Move rule to other Objects.

Unknown Process Filter

To reduce the noise in Unknown Process detection, EventTracker now provides an option " **Unknown Process Filter** " which will help the user in categorizing the process as safe, based on the meta-data of the process.

The user can create specific rules based on the attributes provided in the wizard and can filter out the safe processes.

- New Benchmark added: **DISA**: **Windows 10** and **Microsoft**: **Windows 10**.
- New Reputation service provider “**Borderware**” included in Attackers/Targets Dashboard.

Minor Improvements

Attackers dashboard: Option to customize the Map by theme colors.

Search Around option in **Advanced -> User Preference** will help the user in specifying the time range to search around a particular event property.

Change Audit: Change Audit now supports the monitoring of a specific registry path on a group of systems. It also supports the sending of snapshot files at scheduled intervals.

Log Search: Now the user can view the search results of a specific refine level in Log Search. Links have been provided for each refine level. The user can easily navigate to the desired refine level by clicking the link.

Manager Configuration: In **Admin -> Manager**, option has been provided to configure ETHoneynet URL.

Attackers/Targets Dashboard: The dashboard will populate data based on the default chosen service provider. And once the user changes the service provider, the initial data will be intact and will continue populating data based on the new service provider, for the new IPs.

- **Updated Alerts**
  - ❖ Cisco Sourcefire: High priority alert generated

- **Updated Flex Reports**
  - ❖ EventTracker-USB or other removable media insert-remove
  - ❖ EventTracker-New enterprise activity
  - ❖ EventTracker-Out of ordinary activity
  - ❖ EventTracker-Browser connecting to non-standard port
  - ❖ EventTracker-Non-Browser connecting to port 80 or 443
  - ❖ Windows-System shutdown-restart
  - ❖ Windows-User logon failure
  - ❖ Windows-User logon success
  - ❖ VMware vCenter-Host added or removed
  - ❖ VMware vCenter-Virtual machine created or removed
  - ❖ VMware ESXi-Account created or removed
  - ❖ Centrify Windows Agent-Run as role failed attempts

- Trend Micro InterScan-Trust URL added to exception
- SonicWALL Firewall-Attacks detection
- SonicWALL Firewall-Intrusion detection
- SonicWALL Firewall-VPN activity
- SonicWALL Firewall-VPN User authentication failed
- Cisco ASA-Connection denied
- Cisco ASA-Attack detection
- Windows-Administrative activities
- Cisco IOS-User logon failure
- Cisco IOS-User logon success
- Cisco IOS-Configuration changed
- Cisco Sourcefire-Inbound and outbound traffic
- Cisco Sourcefire-Correlation events
- Cisco Sourcefire-Alert analysis
- Cisco SourceFire-IDS and IPS activity

- **Updated Categories**
  - Cisco Sourcefire: Correlation events
  - Cisco Sourcefire: IPS activity
  - Cisco Sourcefire: Inbound and outbound traffic