EventTracker
Secure. Comply. Succeed.

Feature List

EventTracker v8

Publication Date: Oct. 7, 2015

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 8.0.

Target Audience

EventTracker users who wish to know about the new features added in EventTracker Enterprise v8.0 version.

Table of Contents

Major improvements in v8.0

- EventTracker v8.0 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 with icons.

- New benchmarks that are included:

1) Microsoft

- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11
- Office 2013
- Windows 8.1
- Windows 2012 R2

2) DISA

- Windows 8

- **New Threat Intelligence Pack are included:**

  - **Detect Known-Bad and Unknown process**

  EventTracker alerts IT/Security administrators whenever any new process is executed on windows systems in the network which is not a part of known exe list in the database. It provides detailed information about Process such as Process name, File path, User name, Domain name, Logon ID, Process ID and System name, where new process is executed.

  http://www.eventtracker.com/wp-content/support-docs/How-to-Detect-Known-Bad-and-Unknown-Process.pdf

  - **Bad IP Reputation Lookup**

  EventTracker alerts IT/Security administrators whenever any network activity is detected in network from or to IP address which has bad reputation score. It provides detailed information about Local system, Port, Process, User and Remote IP address with detailed description of the log where bad reputation IP connection is detected.

  http://www.eventtracker.com/wp-content/support-docs/EventTracker-Configure-IP-Reputation-Lookup.pdf

- **Emerging Threat Blocked IP List Import**

Emerging Threats blocked IP list contains the SPAM source or top attackers' source IP addresses from different sources which is downloaded by EventTracker.

EventTracker's IP activity monitoring feature extracts the IP addresses from all the logs received into EventTracker in real-time and allows users to lookup the IP address against the downloaded IP address list from Emerging Threat. This helps EventTracker users to detect any network communication happening from such known vulnerable IP addresses.

http://www.eventtracker.com/wp-content/support-docs/How-to-Configure-Emerging-Threat-Blocked-IP-List-Import.pdf

- **Iblocklist BlueTack Bogon IP List Import**

Blutack Bogon IP list contains the unallocated address space which is downloaded by EventTracker.

EventTracker's IP activity monitoring feature extracts the IP addresses from all the logs received into EventTracker in real-time and allows users to lookup the IP address against the downloaded Bogon IP address list. This helps EventTracker users to detect any network communication happening from such known IP addresses.

http://www.eventtracker.com/wp-content/support-docs/How-to-Configure-IBlocklist-Bluetack-Bogon-IP-List-Import.pdf

- **Iblocklist BlueTack Hijacked IP List Import**

Blutack Hijacked IP list contains the unallocated address space which is downloaded by EventTracker.

http://www.eventtracker.com/wp-content/support-docs/How-to-Configure-IBlocklist-Bluetack-Hijacked-IP-List-Import.pdf

- **IblocklistBlueTackSpyWareListImport**

Blutack Spyware IP list contains the Known malicious spyware and adware IP Address ranges which is downloaded by EventTracker.

http://www.eventtracker.com/wp-content/support-docs/How-to-Configure-IBlocklist-Bluetack-Spyware-List-Import.pdf

- **IblocklistBlueTackProxyIPListImport**

Blutack Tor and proxy IP list contains the known Tor and proxies IP address list which is downloaded by EventTracker.

http://www.eventtracker.com/wp-content/support-docs/How-to-Configure-IBlocklist-BlueTack-Proxy-IP-List-Import.pdf

- New Behavior rule added:

  - **Windows Network Processes**
  - **Windows Network Connections**

- Added a new default behavior rule '**Windows user location affinity**" to detect interactive user logon pattern with respect to a workstation.

- Added a new default behavior rule '**Unique process hash**" to track hash of the process image file.

- **Dashboard>Custom Dashboard**: This option helps to view quick statistics and graphs like trend of events based on any flex persisted data. The custom dashboard is an enhanced feature of the flex dashboard, where the dashboard can be configured as well as customized according to user preferences. The user can now plot various graphs based on the X-axis and Y-axis values available for the reports.

- **Dashboard>Attackers**: Geolocation page to represent bad reputation IPs.

- Ability in behavior engine to consider the combination of activity name and breakup name as a new activity instead of activity name itself for custom rules.

- Support for blocking various new types of USB devices like tablets, mobile phones etc.

- Threshold based monitoring of handle and thread usage of the system and a running process.

- Support for transferring cabs from collection point on scheduled basis.

- Support for extracting field names from header of log file in Direct Log Archiver.

- In **Change Audit**,
  - Ability to create rules for enabling checksum tracking.
  - Sending snapshots to manager can be disabled.
  - The manager name can be configured remotely.
  - Checksum tracking is enabled by default for all executable files (*.exe, *.dll etc.).

- Knowledge Packs - http://www.eventtracker.com/knowledge-center/

  - Barracuda SSL VPN
  - Dell Force 10 Switch
  - Sophos UTM
  - Sonicwall UTM
  - Syslog
  - Snort
  - Amazon Web Services

- Apache Web Server
- Dell Force 10
- eDirectory
- F5 BIG IP ASM
- Juniper JUNOS
- Juniper Netscreen
- Microsoft Windows RRAS
- Ruckus Wireless ZoneDirector
- Sophos Enterprise Console
- Windows
- OKTA SSO
- Palo Alto Firewall
- Red Hat Enterprise Linux
- Fortigate Firewall
- FortiAnalyzer

❖ **ETVAS8- Managing Vulnerability**

- Access Control:
  The access control features were comprehensively extended.

  - Groups: For access permissions users can now be associated with Groups. The web interface allows full management of these groups for users with Administrator role.
  - Roles: Roles are now freely configurable and users can be associated with roles. A new pre-configured role "Info" was added.
  - Permissions: Under menu "Configuration" there is now a new item "Permissions". Here the user has a comfortable overview on all of his access permissions and opportunities to manage them.
  - Roles can now be dynamically configured.
  - New default roles "Monitor", "Guest" and "Super Admin".
  - New Permissions "Super" that allows for example to define an administrator for a group.

- Results are now an explicit part of the scan management.

  The new section "Results" under menu "Scan Management" offers an object management for all of the scan results in the database a user has permission for. In other words, searching and filtering for results is now possible independent of a scan report.

- Solution Type:

  NVTs are now associated with a solution type like for example "VendorFix". This allows to group or identify NVTs or results where for example a simple solution exists or no solution is currently available.
  The Feed content is updated over time to add a solution type for all of the NVTs. At the time of writing, 3.6% of the NVTs own a Solution Type.

- Quality of Detection (QoD):

  The QoD is a value between 0% and 100% describing the reliability of the executed vulnerability detection or product detection.
  One of the main reasons to introduce this concept was to handle the challenge of potential vulnerabilities properly. The goal was to keep such in the results database but only visible on demand.
  New SecInfo object type "CERT-Bund" introduced: These are advisories published by the German federal CERT.

- Credentials:

  - The public key of SSH credentials is not required anymore because it is extracted from the private key.
  - Credentials for ESXi target systems can now be configured directly with the Target object instead of in the Scan Configuration object.
  - When a task is requested to stop, the scanner will now be advised to switch immediately into the final phase of scanning. Activity and did not return so far collected host details. With OpenVAS-8 this is now transferred to the the database.
  - Dropped support for pausing of tasks entirely (was removed from GUI before, now removed from OMP level).

- OpenVAS Scanning Protocol (OSP):

  This new protocol allows to control the vulnerability scanner. The main elements are to set parameters, start a scan and retrieve results. OSP is designed in the same way as OMP, therefore it is a non-permanent request-response connection based on XML.
  It is possible to configure and control OSP-compliant Scanner via the user interface.

Vulnerability Scanning:

- Alive-Test (Up-Test, Ping-Test): The type of test that determines whether a system is active is now adjustable as a property of the object "Target". Which means it can be changed without the need to change Tasks or Scan Configurations. Possible methods are the same as before: ICMP, TCP and ARP.

  The default setting for the Alive-Test changes from ICMP&TCP&ARP to just ICMP. Hence it can happen that results change for some of your Tasks because some

systems are not regarded as alive anymore. But in most cases where larger IP ranges are scanned the scan duration will significantly drop down while getting the same results. However, you do not need to change a Scan Configuration or Task to get back to the previous state; you just need to adjust the Alive-Test method for the respective Target.

- New pre-configure Scan Configuration "Host Discovery". This Scan Configuration simply searches for real systems for the given target addresses. No vulnerability tests are executed. The result is just a list of hosts that are regarded active.
- New pre-configure Scan Configuration "System Discovery". This Scan Configuration applies any NVTs that discover operating system types and/or hardware device types. No vulnerability tests are executed. The main result is an overview on the found operating system and devices.
- New pre-configure Scan Configuration "Discovery". This Scan Configuration applies any NVTs that discover as many details about the target system, installed services and applications, as possible. No vulnerability tests are executed.
- Tasks: New class "Alterable Task" allows to change the Target and Scan Config even if there are already reports for this task. This allows to have a playground task not designed to grant consistency between its reports.
- Problems with DNS resolving during scan: Each failed resolving of a target system name is now listed in section "Errors" of the report browser.

Graphical User Interface:

- Dynamic charts are introduced, using the Javascript library "d3". The first chart types (bar, donut, bubbles, line) are used for the SecInfo section in order to demonstrate some of the capabilities.
- The chart object allows to download the data as CSV table or SVG graphics. Also, a HTML table can be opened and some of the charts are interactive.
  For the SecInfo Management, a first dashboard is integrated which assembles four of the charts and can be configured individually.
- The charting feature is entirely optional: Without enabling Javascript support in the browser no core functionality is lost. Also, the chart view can be collapsed so that only the traditional table view is shown.
- Timezones:
  The configuration of timezones was changed so that now there is offered a drop down list of available timezones instead of a entry field for specifying the timezone in text form.
- Users are now allowed to have multiple simultaneous sessions, as long as the sessions are on different browsers.
- For any web interface page, the duration of the backend operation will be shown at the bottom.
- New wizard for modifying a task.

Architecture:

- redis (mandatory):
  The OpenVAS Scanner now uses a redis backend to share the knowledge base among the scanning processes.
- The memory consumption of the OpenVAS Scanner was reduced by about 50%.

❖ **ETIDS8**

- ➢ Snort version included in ETIDS is Snort 2.9.7.2
- ➢ Emerging Threat open rules for snort is used by default.
- ➢ Option to use Emerging Threat Pro rules with snort (customer require to subscribe for same.

❖ **Agent Filters added (Workstations)**

- Added default Advanced filters to drop event ids 560, 565 & 566 of Log Type "Security" with $ user.
- Added default Advanced filter to drop event id 560 of Event Type "Audit Success" with description "$Window||.tmp||$$_||~"
- Added default Advanced filters to drop event ids 3225 & 3404 of source "EventTracker".
- Added default Advanced filter to drop event id 4100 of source "Microsoft-Windows-PowerShell"
- Added default Advanced filter to drop event id 4673 of source "Microsoft-Windows-Security-Auditing".
- Added default Advanced filters to drop event ids 4660, 4661, 4662, 5136, 5137, 5138 & 5139 of source "Microsoft-Windows-Security-Auditing" with description "$</Data><Data Name='SubjectDomainName'>".
- Added default Advanced filter to drop event id 4656 & 5145 of source "Microsoft-Windows-Security-Auditing" with description "$Window||.tmp||$$_||~||$</Data><Data Name='SubjectDomainName'>.
- Added default Advanced filter for event ids 3221 and 3222 of source "EventTracker" to drop events with description containing "sendtrap.exe" or "powershell"

❖ **Agent Filters added (Server)**

- Added default Advanced filter for event id 1002 of source "Microsoft-Windows-KnownFolders" with description "occurred while verifying known folder".

- Added default Advanced filter for event id 3404 of source "EventTracker"
- Added default Advanced filter for event id 4100 of source "Microsoft-Windows-PowerShell"
- Added default DLA filters to drop event ids 528, 538, 540, 560, 565 & 566 of Log Type "Security" with $ user.
- Added default DLA filter to drop event id 560 of Event Type "Audit Success" with description "$Window||.tmp||$$_||~"
- Added default DLA filters to drop event ids 3225 & 3404 of source "EventTracker".
- Added default DLA filter to drop event id 4100 of source "Microsoft-Windows-PowerShell"
- Added default DLA filter to drop event id 4673 of source "Microsoft-Windows-Security-Auditing".
- Added default DLA filters to drop event ids 4660, 4661, 4662, 5136, 5137, 5138 & 5139 of source "Microsoft-Windows-Security-Auditing" with description "$</Data><Data Name='SubjectDomainName'>".
- Added default DLA filter to drop event id 4656 & 5145 of source "Microsoft-Windows-Security-Auditing" with description "$Window||.tmp||$$_||~||$</Data><Data Name='SubjectDomainName'>.
- Added default DLA filter for event ids 3221 and 3222 of source "EventTracker" to drop events with description containing "sendtrap.exe" or "powershell"

❖ **Agent Network Connection Module**

The Agent Network Connection Monitoring module is updated to use real-time trace. The updated network connection monitoring module generates events in range 3512-3516 instead of events in range 3223-3227.

❖ **News Dashboard**

The news dashboard will display the Product announcements, news and Local broadcast messages by EventTracker user.

❖ **Targets dashboard**

With the advent of the new feature 'Attacks Dashboard" where the bad reputation IPs are pinned on the geolocation, it becomes necessary to display the information as to where these bad IPs have ventured in to the network. The targets dashboard feature will suffice the requirement, displaying those targets within the enterprise which are being attacked,

along with the details like-How (Port/Protocol), By Whom (IP/Host Name) and When/ How often.

- **Enhancement in the feature: Export Import Utility**

  For Reports the user can now export/import either Legacy/New type for Scheduled/Defined reports option. For the new type the valid extension is *.etcrx.

- **Manager> Direct Log Archiver**

  Date and Time parsing support has been enhanced in Direct Log Archiver (For Types: Others and Log).

- **Agent Configuration>Processes>Advanced**

  The Specific Processes feature will provide individual CPU and Memory threshold for Specific processes.

Minor improvements

- Additional parameters including incident number are passed to "Console Remedial Action" script.
- An Option to disable storage of notification status for an alert.
- In **Export Import Utility**: Export/Import the category/alert/filter/behavior rule, if rule contains Logtype, Eventtype**.**
- In **Admin>Windows Agent configuration**: Option to provide custom port in agent configuration.
- Agent Templates feature enhancement with new option: **Load Template**.
- DLA now includes **XML** and **LOG4XML** format log files.
- Reports/web modules: The Excel reports theme is changed.
- Reports Wizard: Allow user to set Run time for scheduled reports.
- Network connection monitoring is enabled by default for new TCP connections.
- XML event description of windows events is by default included in the description.

- Notification when an Agent stops reporting and starts reporting again (Enhancement in Agent Health Check monitoring.)

- Ability to initiate remedial actions (like run scripts, kill process, add firewall rule etc) from the Console on remote agent system.

- Added new option in **Diagnostics** utility to provide disk space threshold.
- The feature StatusTracker has been moved to the **Tools** menu.

- If the **ETIDS** is availed in the license, the user will be able to view the option under the **Tools** menu. The option will help the user to connect to ETIDS (Integrated with Snorby).

- Option providing custom parameters in scheduled scripts for **Attacks** and **Targets** report.

- In **Parsing Rules**, grouping for token templates has been provided.

- In **Behavior**, for IP Address Activity, log Search option has been provided for All/ Behavior.

- Support has been provided for considering 3512 and 3513 for Network Monitoring in behavior. Notification is added for new IP Pair detection in **Behavior**.

- **Updated Categories**

  - BIG-IP LTM: ARP entry deleted
  - BIG-IP LTM: ARP static entry
  - BIG-IP LTM: Authentication failed
  - BIG-IP LTM: Authentication success
  - BIG-IP LTM: Configuration failed
  - BIG-IP LTM: Connection error
  - BIG-IP LTM: Member unavailable for pool
  - BIG-IP LTM: Monitor created
  - BIG-IP LTM: Monitor removed
  - BIG-IP LTM: New node added
  - BIG-IP LTM: New route addition failed
  - BIG-IP LTM: New route addition success
  - BIG-IP LTM: New SNAT added
  - BIG-IP LTM: NTP server configured
  - BIG-IP LTM: Packet filtering disabled
  - BIG-IP LTM: Packet filtering enabled
  - BIG-IP LTM: Packet filtering rule modified
  - BIG-IP LTM: Pool member creation failed
  - BIG-IP LTM: Pool member creation success
  - BIG-IP LTM: Pool member deleted

- BIG-IP LTM: Pool member status down
- BIG-IP LTM: Pool member status up
- BIG-IP LTM: Remote server added
- BIG-IP LTM: Root login failure
- BIG-IP LTM: SNMP agent configured
- BIG-IP LTM: System shutdown
- BIG-IP LTM: User account deleted
- BIG-IP LTM: User account modified
- BIG-IP LTM: Virtual server created
- EventTracker: Network Connections
- Watchguard XTM: Firewall allowed traffic
- Watchguard XTM: Firewall denied traffic

❖ **Updated Alerts**

- BIG-IP LTM: ARP entry deleted
- BIG-IP LTM: Authentication failed
- BIG-IP LTM: Authentication success
- BIG-IP LTM: Connection error
- BIG-IP LTM: Monitor removed
- BIG-IP LTM: Packet filtering disabled
- BIG-IP LTM: Packet filtering rule modified
- BIG-IP LTM: Pool member status down
- BIG-IP LTM: Root login failure
- BIG-IP LTM: User account deleted
- Critical Potential Breach: A New Process Connecting to Low Reputation IP Address
- Critical Potential Breach: Unknown Process Connected to a Bad Reputed Remote Site Across Firewall
- Disk space is Critically Low on EventTracker Server
- EventTracker: New IP Activity Reputation Lookup
- EventTracker: Connection to Bad IP Reputation Process Lookup
- EventTracker service down
- High CPU Utilization on EventTracker Server
- NCM-Browser Connecting to Non Webserver Port
- NCM-Non Browser EXE Connecting to Known Webserver Port
- Windows: Audit log cleared

❖ **Updated Flex Reports**

- Snort-Alert Analysis
- Windows-Administrative Activities
- Windows-AD Object Access Detail Report

- NCM - All New Network Connection Report
- NCM-Browser Connecting to Non Webserver Port
- NCM-Non Browser EXE Connecting to Known Webserver Port
- Palo Alto Firewall - Threat Details
- Palo Alto Firewall - Traffic Details
- SonicWALL - AntiSpam Service Enabled or Disabled
- SonicWALL - Multicast Policy Added or Deleted
- SonicWALL - System Shutdown by Administrator
- SonicWALL - Terminal Service and SSO Agent Down