EventTracker
Secure. Comply. Succeed.

Monitor Important Windows Security Events using EventTracker

White Paper

Publication Date: Mar 14, 2014

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

Abstract

Monitoring the Windows security is critical because the Operating System continuously monitors and logs critical security, system and application events in the Windows Security Log.

This guide will easily and efficiently help you in configuring the most important windows security events.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.x and **all flavors of Windows operating system**.

Intended Audience

EventTracker users who are assigned the task to monitor and manage events using EventTracker.

Table of Contents

Windows Security Challenges

Safeguarding windows is absolutely necessary to refrain against cyberpunks, for detection of network outages and protocol failures and to detect the failed processes, services and batch jobs. To proactively troubleshoot windows in production environment and prevent data being breached. Windows security is crucial for business productivity as security breaches can be calamitous. To forbid the disruption of Windows against malware and desist being targeted by hackers, security of Windows plays a prime role so that end users can breathe a sigh of relief.

In most Windows environments audit logs are underutilized. They are often examined only for investigation purposes and usually after an incident. However Windows logs, when properly configured and efficiently monitored, have tremendous value. System logging generates vast amount of data from varying sources. As a result, the process of consolidating, inspecting and analyzing them may be tedious and inefficient. The challenges are compounded by inadequate configuration resulting in logs being full, overwritten, incomplete and useless.

How to monitor Windows Security?

Auditing for security events on critical computer systems is an essential requirement of a sound security policy. A Windows audit policy defines which security events have success and/or failure actions audited and recorded in the Security log.

Critical Windows Security Events

Some of the critical windows security events are grouped and it has to be monitored regularly to ensure that the operating system is intact and they are

- Audit integrity
- System security
- Admin authority
- Logon/authentication failures
- Certificate authority

- Misc

Audit integrity

- **1102 Audit log was cleared -** Event 1102 is logged whenever the Security log is cleared, Regardless of the status of the Audit System Events audit policy. The Account Name and Domain Name fields identify the user who cleared the log.
- **4719 Audit policy changed -** This computer's system level audit policy was modified - either via Local Security Policy or Group Policy in Active Directory. According to Microsoft, this event is always logged when an audit policy is disabled, regardless of the "Audit Policy Change" sub-category setting. This and several other events can help identify when someone attempts to disable auditing to cover their tracks.

System security

- **4739 Domain policy changed -** This computer's Security Settings\Account Policy or Account Lockout Policy policy was modified, either via Local Security Policy or Group Policy in Active Directory.

  There are few other operations that can generate this event, including:

  - Raising the domain functional level
  - Security option: "Network security: Force logoff when logon hours expire"

- **4704 User right assigned -** This event documents a change to user right assignments on this computer including the right and user or group that received the new right.

  Note: "User rights" and "privileges" are synonymous terms used interchangeably in Windows.

  Rights, like most other security settings, are defined in group policy objects and applied by the computer. Therefore this event will normally show the Assigned By user as the system itself. To determine who actually made the rights assignment change you must search the domain controllers' security logs for changes to groupPolicyContainer objects (logged by Directory Service auditing).

- **4717 Logon Right Granted -** This event documents the grant of logon rights such as "Access this computer from the network" or "Logon as a service".

- **4697 New service installed -** A new service was installed by the user indicated in the subject. Subject often identifies the local system (SYSTEM) for services installed as part of native Windows components and therefore you can't determine who actually initiated the installation.

- **4616 System time changed -** This event indicates the old and new system time as well as who did it as specified in the Subject: section. Process information shows the program that was used to change the time. Changing the time manually from the taskbar uses rundll.exe as shown in the example. It is routine to see this event where subject is "LOCAL SERVICE", process name is "svchost.exe" and can be ignored.

Admin authority

- **Any authentication event for "Administrator"**
  - 4775 An account could not be mapped for logon.
  - 4776 The domain controller attempted to validate the credentials for an account. Member servers and workstations also log this event for logon attempts with local SAM accounts.
  - 4777 The domain controller failed to validate the credentials for an account – Since 4776 is logged for both success and failure, there is no need for this event id.
  - 4768 A Kerberos authentication ticket (TGT) was requested - This event is logged on domain controllers only and both success and failure instances of this event are logged.
  - 4771 Kerberos pre-authentication failed - This event is logged on domain controllers only and only failure instances of this event are logged.
  - 4772 A Kerberos authentication ticket request failed.

- New admin
  - 4728, 4732, 4756 – These events are Active Directory Group membership changes which are logged to the Security eventlog

- And details includes "Admins" or "Administrators"

- Caveat: nested groups
- Caveat: password reset / re-enablement on members of

Logon/authentication failures

- Failed local account logon
  - 4625 An account failed to log on - This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account.
  - Computer Name = Account Domain
- Unusual domain authentication failure
  - 4768, 4771
  - 0xC Workstation restriction or
  - 0x12 Account disabled, expired, locked out, logon hours

Certificate authority

- **4870 Certificate Services revoked a certificate -** When an administrator revokes a certificate the certificate is moved to the Revoked Certificates folder and this event is logged. Reason for revocation noted below.
- **4882 The security permissions for Certificate Services changed -** This event documents a change to the access control list of the Certification Authority itself.
- **4885 The audit filter for Certificate Services changed -** Windows logs this event whenever you modify the Auditing tab of the Properties dialog of the CA in the Certification Authority MMC snap-in. The Audit tab controls which CA related events are reported to the security log.
- **4888 Certificate Services denied a certificate request** - This event is logged if either:

- An administrator or other certificate manager denies a pending request. This event 4888 is logged in addition to 4868. It may even be logged twice with 4868 in between.
- The Certification Authority itself denies the request based on policy.

This event is only logged if "Issue and manage certificate requests" is enabled on the Audit tab of the CA's properties in Certificate Services MMC snap-in and of course if the Certificate Services audit subcategory is enabled with auditpol.

- **4890 The certificate manager settings for Certificate Services changed -** This event is logged when you modify the settings in the Certificate Managers tab of the CA properties dialog in Certification Authority MMC snap-in.
- **4891 A configuration entry changed in Certificate Services -** Windows logs this event to document changes to Certificate Services registry entries many of which correspond to properties in the CA Properties dialog of Certification Authority MMC snap-in.
- **4892 A property of Certificate Services changed**
- **4899 A Certificate Services template was updated -** Having tested for this event by making changes to certificate templates I conclude Windows fails to log this event.
- **4900 Certificate Services template security was updated -** Windows logs this event when you modify the ACL on a certificate template.

Easy steps to quickly and efficiently monitor windows security events using EventTracker

Download the Windows security events category file and import it into EventTracker via EventTracker's Control panel. Use this category file to create reports, log search and also in security dashboard. The detail steps are given below.

Import windows security events knowledge pack into EventTracker

1 Launch **EventTracker Control Panel**.

2 Double click **Import Export Utility**, click the **Import** tab.

3 To import category, click **Category** option, and then click the **browse**  button.

4 Locate the Windows Security.iscat file, and then click the **Open** button.

5 Click the **Import** button to import the categories.

6 To import alerts, click **Alerts** option, and then click the **browse**  button.

7 Locate the Windows Security.isalt file and then click the **Open** button.

8 Click the **Import** button to import the alerts.

Configure Security Dashboard using imported category

1. Logon to EventTracker Enterprise.
2. Select the **Dashboard** menu and then select **Security**.
3. To configure **Security Dashboard**, select **Security** drop down, and then select **Configure**.

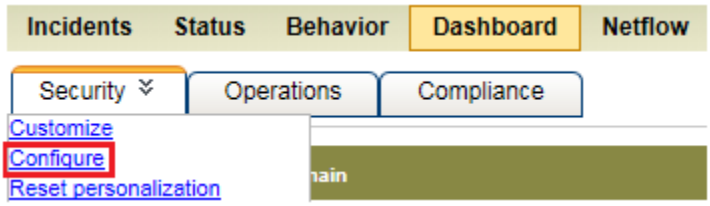


Figure 1

Configure Dashlets window displays.

4. Enter **Title** of the dashlet.
5. Select **Category** tab and **Search for** the category **Windows Security**.
6. Select **Systems** icon and search for the selected systems.
7. Click the **Configure** button.
8. Select **Security** drop down, and then select **Customize**.

   Available dashlets window displays.

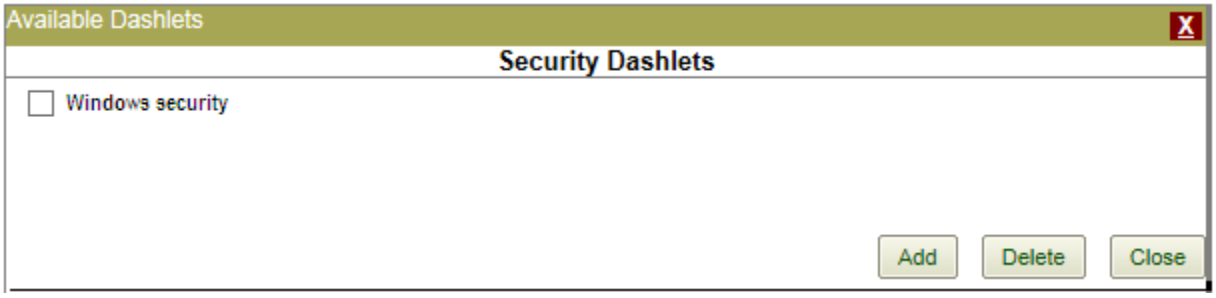


Figure 2

9. Select **Windows security** option, and then click the **Add** button.

   The respective details display in Security dashlet.

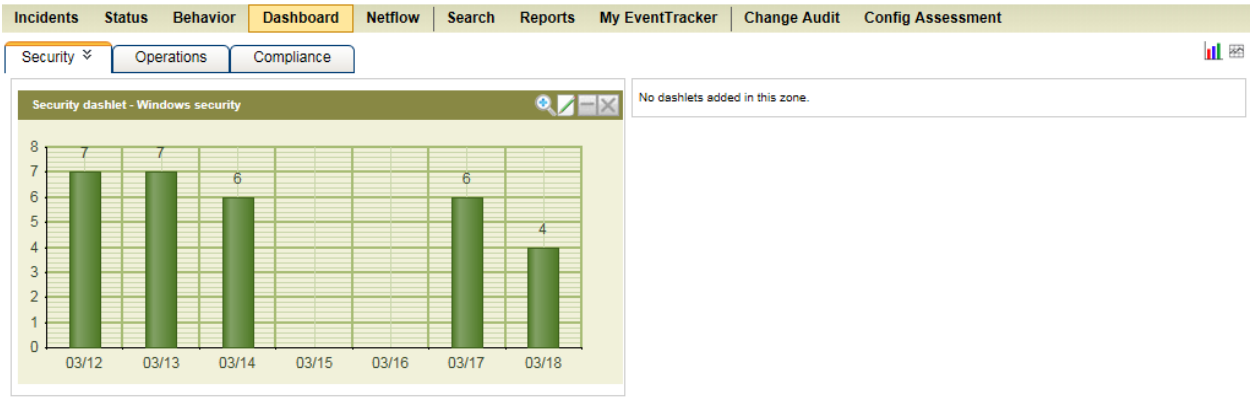


Figure 3

Execute Log Search from an imported category

1. Logon to EventTracker Enterprise.
2. Select the **Search** menu.

   Log Search window displays.
3. In the right pane, expand **All categories** node.
4. Scroll down and expand **Windows** node.
5. Select **Windows security** and then select the **Go** button.

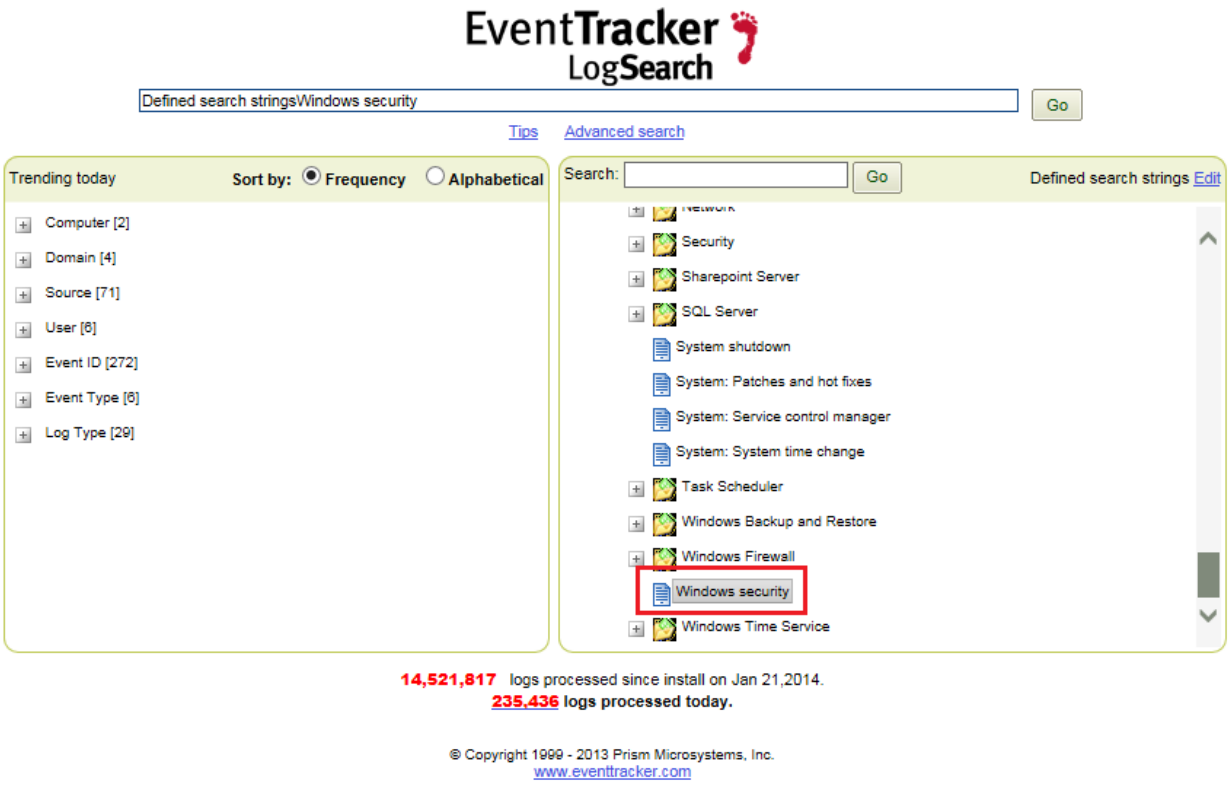


Figure 4

The resultant output displays.

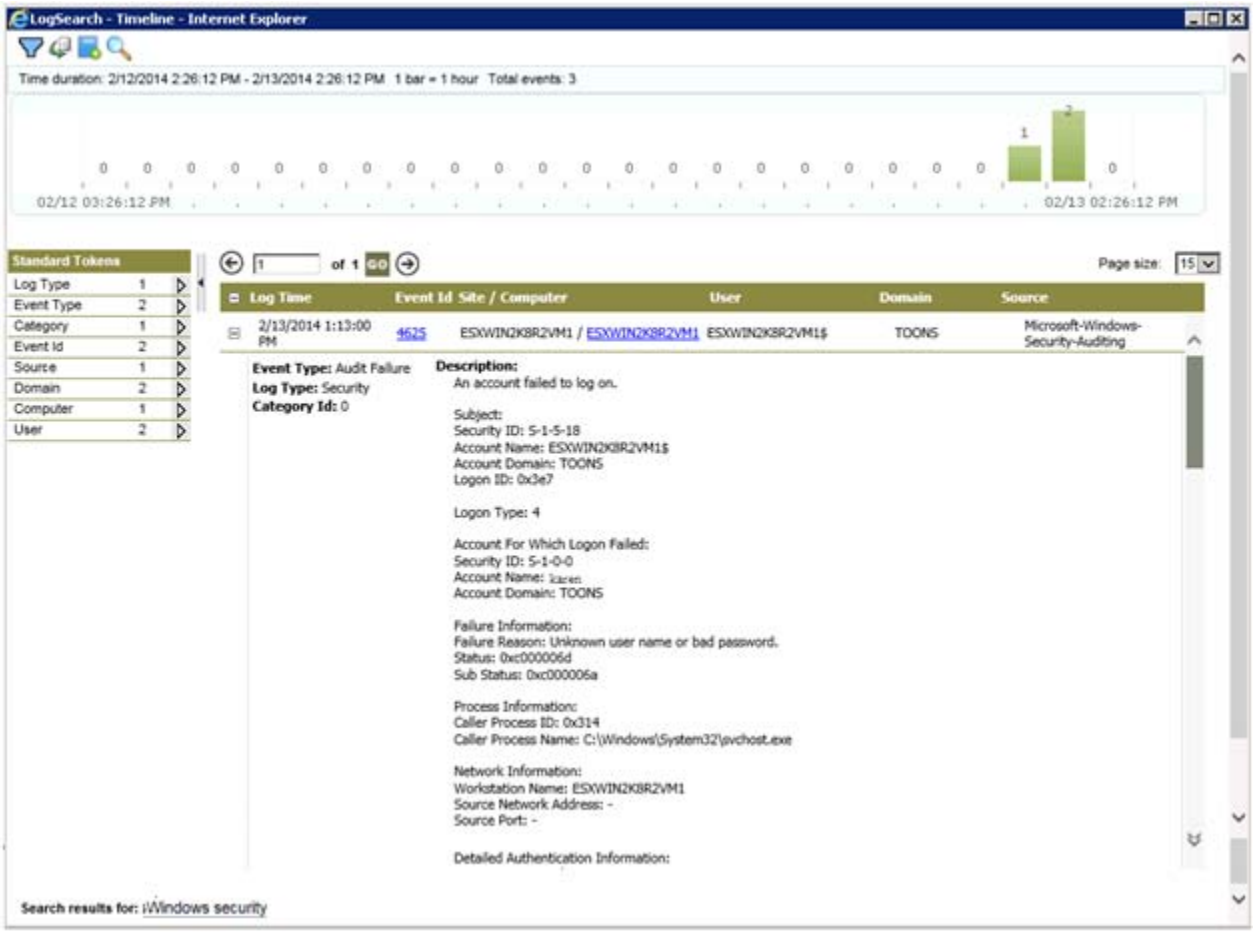


Figure 5

Schedule a report from an imported category

1 Logon to **EventTracker Enterprise**.

2 Click the **Reports** menu and then select **Dashboard**.

3 In the **Reports Dashboard** pane, click the **New** button.

EventTracker :: Reports window displays.

4 Select **Operations** tab, and expand **Windows** group.

5 Select the imported category – **Windows security**, and then click the **Scheduled** button.

Reports Wizard displays.

6 Click the **Next >>** button.

7 Select the '**Groups/Systems/All Systems**' for analysis, and then click the **Next >>** button.

8 Select the **Schedule report** and **More options**, and then click the **Next >>**button.

9 Enter **Refine** and **Filter** criteria, and then click the **Next >>**button.

10 Enter **Title** and **description** for the analysis, and then click the **Next >>**button.

11 Crosscheck **Disk cost analysis** details.

12 Configure the **Publishing options** as required, and then click the **Next >>**button.

13 Click the **Schedule** button.

EventTracker displays message box.

Benefit of SIEM Simplified Services

SIEM Simplified is our professional services engagement to enhance the value of the EventTracker Enterprise and EventTracker Security Center products. Our experienced staff assumes responsibility for all SIEM related tasks including daily incident reviews, daily/weekly log reviews, configuration assessments, incident investigation support and audit support. We augment your IT team, allowing you to remain focused on the unique requirements of your enterprise while actively leveraging our expertise. Our team will take the responsibility of configuring relevant reports, alerts, log search and in security dashboard and finally notify customers with the summary report.

Sample Analysis report

Category Summary Report Sorted By Computer — **EventTracker Report** / **EventTracker**

Quick View

This report gives you information on the selected Categories in your enterprise. The report can be used to track system activity in relation to a Category thereby giving you an insight into the security and other implications.

From Date : 2/9/2014 6:13:58PM

To Date : 2/10/2014 6:13:58PM

Total number of Computers monitored are 1

Limit Time Range: None

Computers Selected: All Systems

Categories Selected: Windows security

Refine: None

Filter: None

Description: None

Sites selected: MCLOON, Alice

Top 1 Categories with Top 1 Computer's

Windows security

Category	Category Description	Computer	No. Events
Windows security	This category provides information regarding 27 most security events to monitor.	1	10

Category Summary Report Sorted By Computer

EventTracker Report
EventTracker

Category Summary Report Sorted By Computer

Category Windows security had 1 Computers generating 10 events

Event IDs included are 4625

Computer	No. Events
MCLOON\MCLOON	10

Total number of Computers monitored are 1

Limit Time Range: None

Computers Selected: All Systems

Categories Selected: Windows security

Refine: None

Filter: None

Description: None

Sites selected: MCLOON, Alice

Detail Report

Category Detail Report Sorted By Computer

EventTracker Report
EventTracker

Quick View

This report gives you information on the selected Categories in your enterprise. The report can be used to track system activity in relation to a Category thereby giving you an insight into the security and other implications.

From Date : 2/5/2014 4:32:44PM

To Date : 2/12/2014 4:32:44PM

Total number of Computer(s) where event has occured 1

Limit Time Range: None

Computers Selected: All Systems

Categories Selected: Windows security

Refine: None

Filter: None

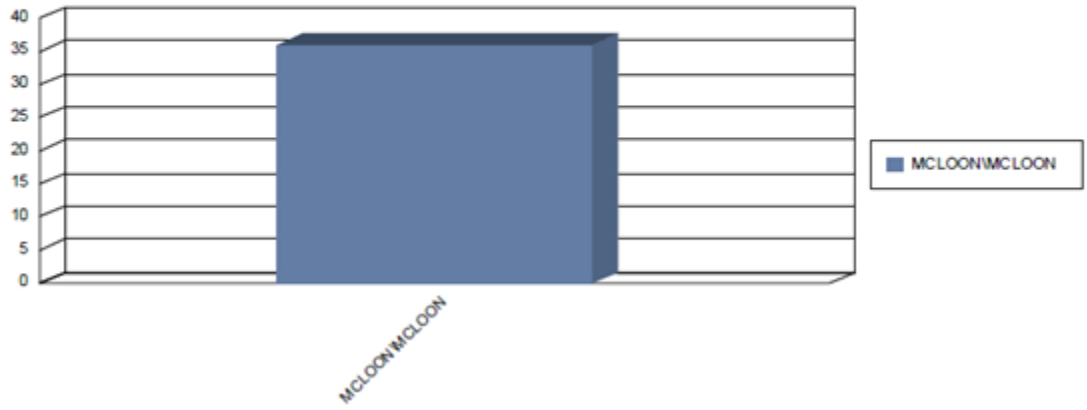
Description: None

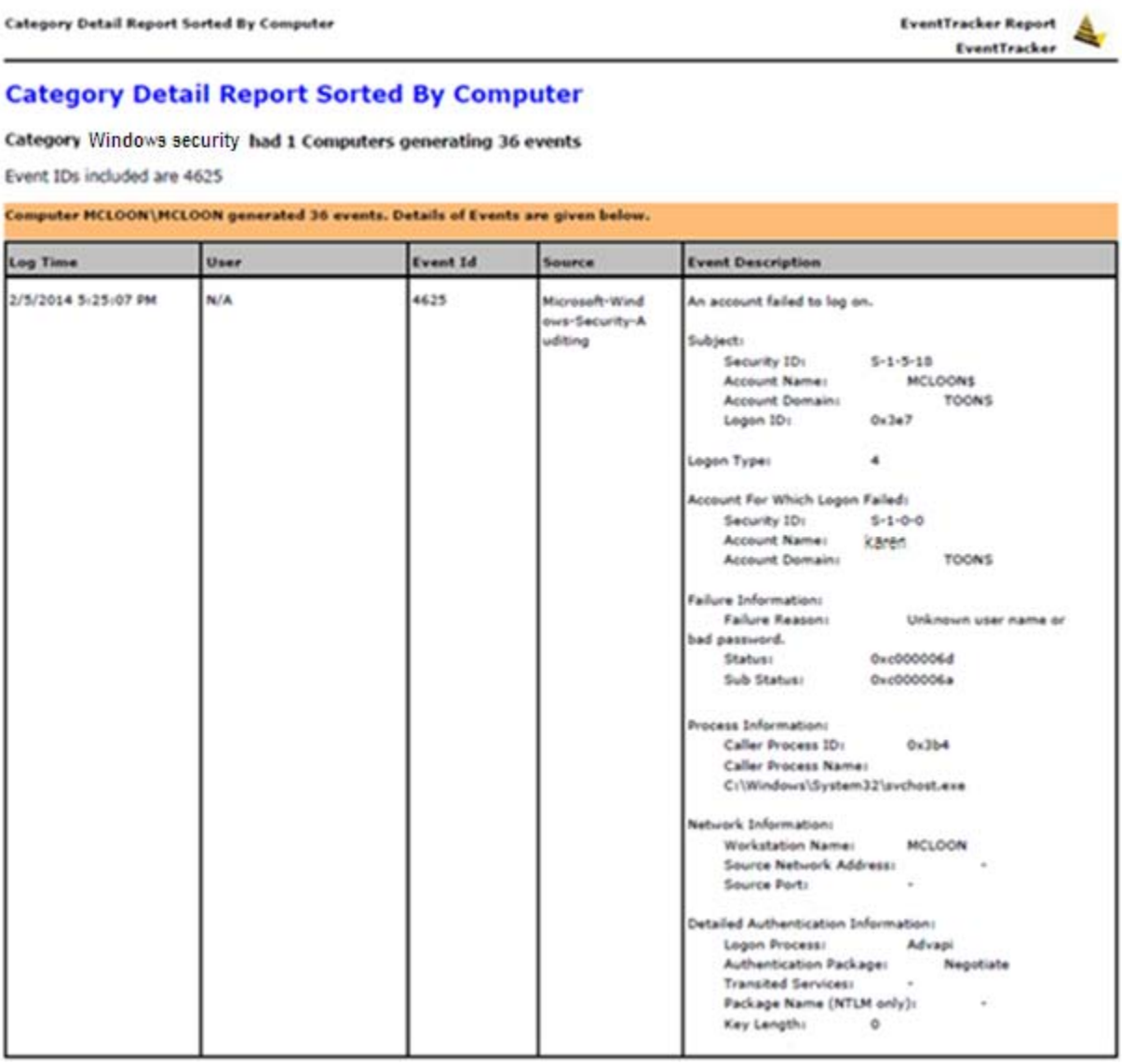
Sites selected: MCLOON, Alice

Category	Category Description	Computer	No. Events
Windows security	This category provides information regarding 27 most security events to monitor.	1	36

Top 1 Categories with Top 1 Computer's

Windows security





Category Detail Report Sorted By Computer

EventTracker Report
EventTracker

Category Detail Report Sorted By Computer

Category Windows security **had 1 Computers generating 36 events**

Event IDs included are 4625

Computer MCLOON\MCLOON generated 36 events. Details of Events are given below.

Log Time	User	Event Id	Source	Event Description
2/5/2014 5:25:07 PM	N/A	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: MCLOON$ Account Domain: TOONS Logon ID: 0x3e7 Logon Type: 4 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: karen Account Domain: TOONS Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xc000006d Sub Status: 0xc000006a Process Information: Caller Process ID: 0x3b4 Caller Process Name: C:\Windows\System32\svchost.exe Network Information: Workstation Name: MCLOON Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Advapi Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0