TENABLE NETWORK SECURITY, INC.

File and Directory Modifications

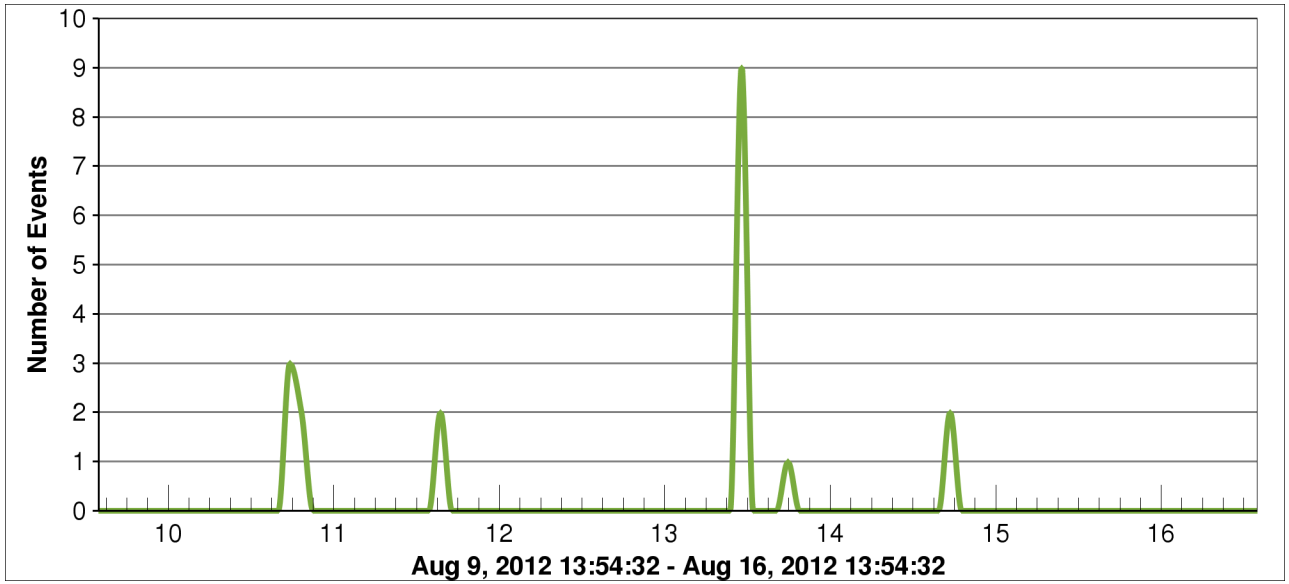
August 16, 2012 at 1:54pm CDT
Dave Breslin [dbreslin]

TENABLE
Network Security®

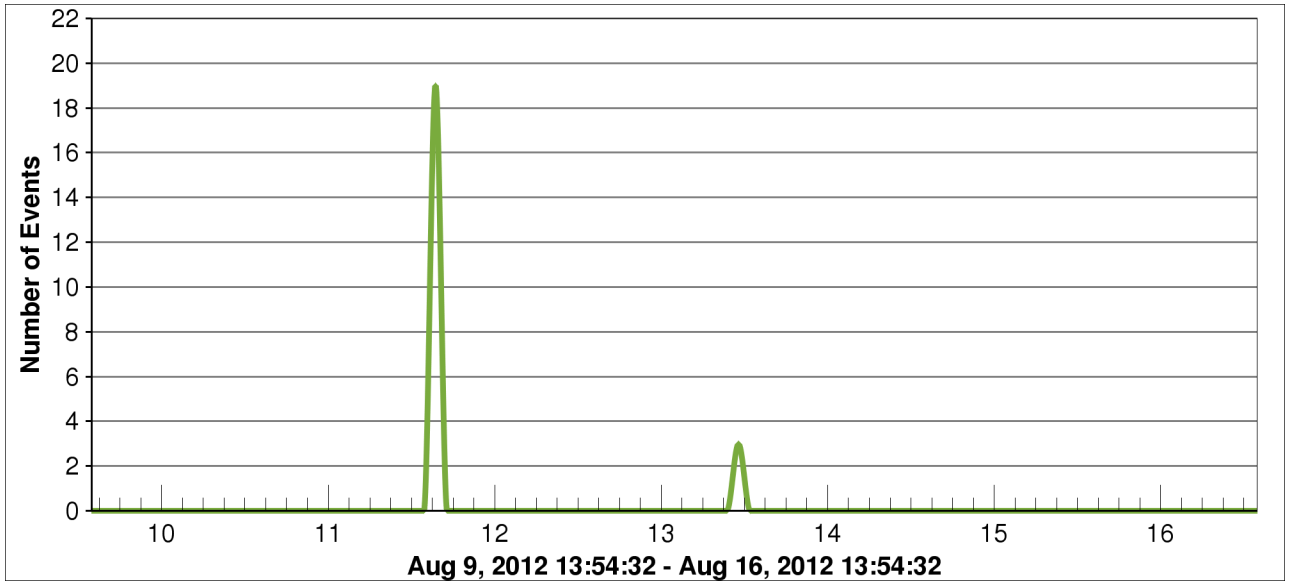
Table of Contents

Summary

File and Directory Change Events (Past 7 Days)



Software Installed Events (Past 7 Days)

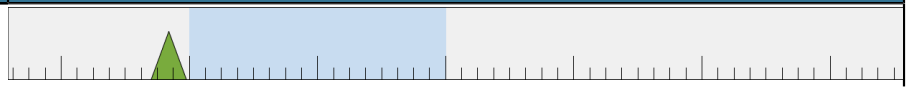
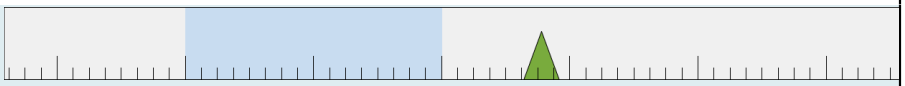
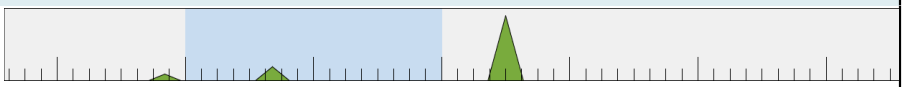
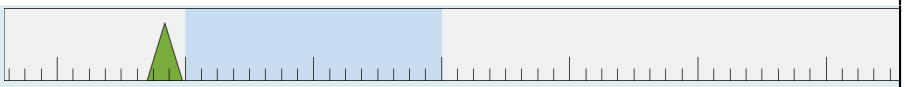
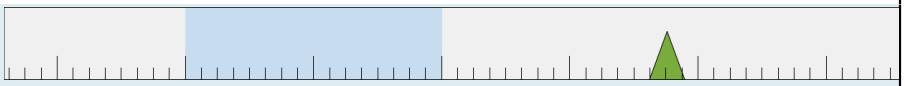
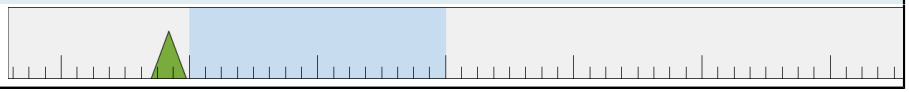


File and Directory Changes by Location (Past 7 Days)

	Count
HQ 2nd Floor	38
HQ 1st Floor	0
HQ 3rd Floor	0
Distribution Center 1	0
Distribution Center 2	0
Distribution Center 3	0
Distribution Center 4	0
HQ Wireless	0
HQ Mgmt	0

Details (Past 7 Days)

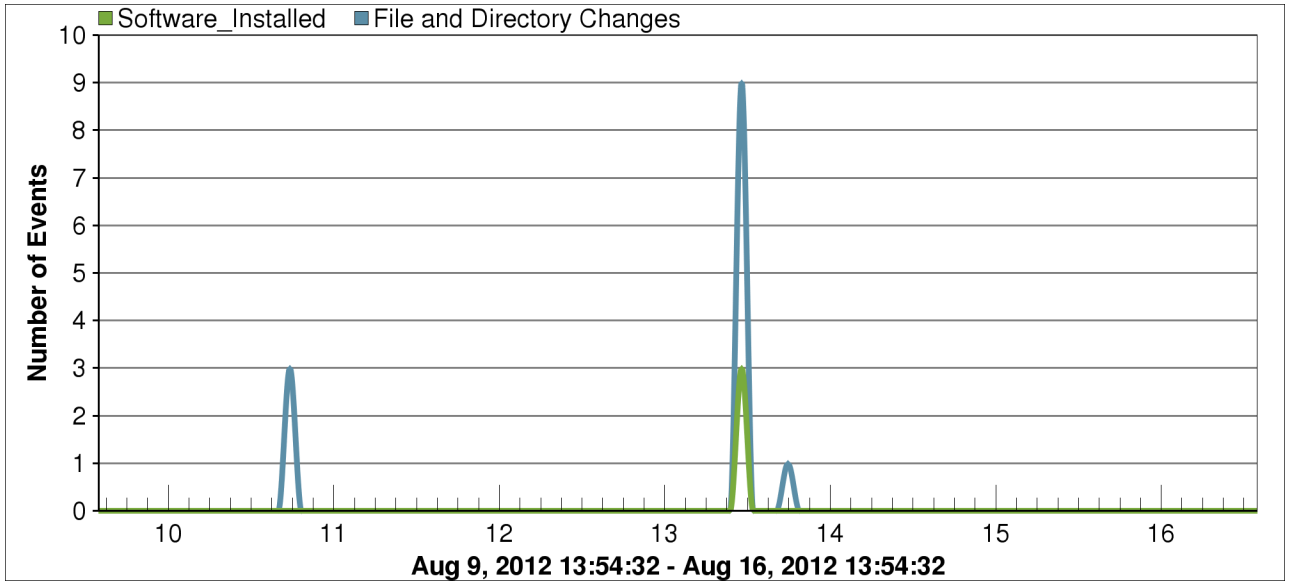
File and Directory Change Events

Event	Count	Aug 9, 2012 13:54:32 to Aug 16, 2012 13:54:32
LCE-Monitored_File_Modified	1	
LCE-Monitored_File_Removed	1	
LCE-New_File_Added_To_Directory	12	
LCE-Unix_Configuration_File_Modified	2	
LCE-Unix_Executable_File_Modified	1	
LCE-Unix_Library_File_Modified	1	
LCE-Unix_Tenable_File_Modified	1	

10.0.0.5

Repository: Credentialed
DNS Name: MM2001.local
Vulnerabilities: Critical: 10, High: 11, Medium: 5, Low: 0, Info: 25
Last Scan: Aug 16, 2012 @ 12:50PM

Host Events



Details (Past 7 Days)

Software Installed Event Details

Time	Message
Aug 13, 2012 10:21:08 CDT	Software_Installed - 8/13/2012 10:21:08 - Evaluated as event OSX-Application_Installed Host: 10.0.0.5
Aug 13, 2012 10:21:08 CDT	Software_Installed - 8/13/2012 10:21:08 - Evaluated as event OSX-Application_Installed Host: 10.0.0.5
Aug 13, 2012 10:21:31 CDT	Software_Installed - 8/13/2012 10:21:31 - Evaluated as event OSX-AdobeFlash_Installed Host: 10.0.0.5

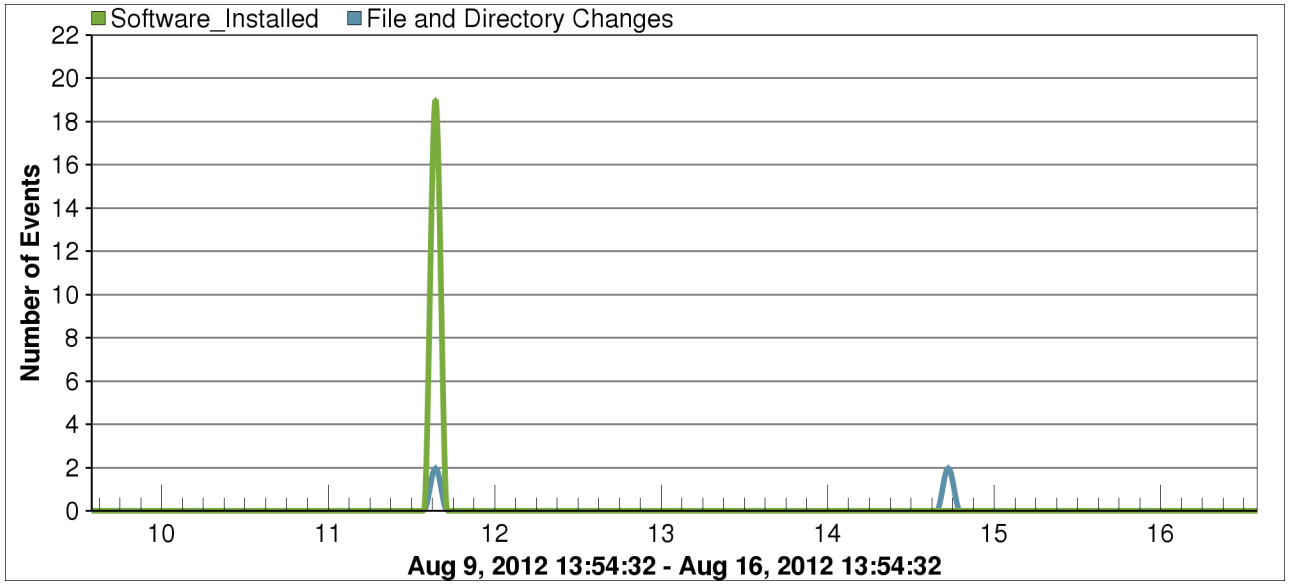
File and Directory Change Event Details

Time	Message
Aug 10, 2012 18:24:48 CDT	New file /etc/tunnel.pl was added to monitored directory.
Aug 10, 2012 18:24:48 CDT	File /etc/sshd_config has been modified. Its permissions changed from 0644 to 0666.
Aug 10, 2012 18:24:48 CDT	File /etc/ssh_config has been modified. Its MD5 checksum changed from 3a25462b244dff21f689df2313b70e2f to dfff01c605bed7b006ad479e5b22af43. Its permissions changed from 0644 to 0666.
Aug 13, 2012 10:44:15 CDT	New file /var/db/receipts/com.adobe.pkg.FlashPlayer.bom was added to monitored directory.
Aug 13, 2012 10:44:15 CDT	New file /var/db/receipts/com.adobe.pkg.FlashPlayer.plist was added to monitored directory.
Aug 13, 2012 10:44:15 CDT	New file /Library/LaunchDaemons/com.adobe.fpsaud.plist was added to monitored directory.
Aug 13, 2012 11:44:25 CDT	New file /etc/ssh_host_dsa_key was added to monitored directory.
Aug 13, 2012 11:44:25 CDT	New file /etc/ssh_host_key was added to monitored directory.
Aug 13, 2012 11:44:25 CDT	New file /etc/ssh_host_dsa_key.pub was added to monitored directory.
Aug 13, 2012 11:44:25 CDT	New file /etc/ssh_host_key.pub was added to monitored directory.
Aug 13, 2012 11:44:25 CDT	New file /etc/ssh_host_rsa_key was added to monitored directory.
Aug 13, 2012 11:44:32 CDT	New file /etc/ssh_host_rsa_key.pub was added to monitored directory.
Aug 13, 2012 18:16:18 CDT	File /etc/tunnel.pl was removed. Its last MD5 checksum was f0c9b744ce9fbfc7e4c4717c09870e26.

10.0.0.6

Repository: Credentialed
DNS Name: MM2003.local
Vulnerabilities: Critical: 0, High: 1, Medium: 2, Low: 0, Info: 27
Last Scan: Aug 16, 2012 @ 12:50PM

Host Events



Details (Past 7 Days)

Software Installed Event Details

Time	Message
Aug 11, 2012 14:43:02 CDT	Software_Installed - 8/11/2012 14:43:02 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:02 CDT	Software_Installed - 8/11/2012 14:43:02 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:12 CDT	Software_Installed - 8/11/2012 14:43:12 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:12 CDT	Software_Installed - 8/11/2012 14:43:12 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:18 CDT	Software_Installed - 8/11/2012 14:43:18 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:18 CDT	Software_Installed - 8/11/2012 14:43:18 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:18 CDT	Software_Installed - 8/11/2012 14:43:18 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:43:22 CDT	Software_Installed - 8/11/2012 14:43:22 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:44:05 CDT	Software_Installed - 8/11/2012 14:44:05 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:44:05 CDT	Software_Installed - 8/11/2012 14:44:05 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:44:05 CDT	Software_Installed - 8/11/2012 14:44:05 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:10 CDT	Software_Installed - 8/11/2012 14:45:10 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:12 CDT	Software_Installed - 8/11/2012 14:45:12 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:13 CDT	Software_Installed - 8/11/2012 14:45:13 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:21 CDT	Software_Installed - 8/11/2012 14:45:21 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:21 CDT	Software_Installed - 8/11/2012 14:45:21 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:24 CDT	Software_Installed - 8/11/2012 14:45:24 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:24 CDT	Software_Installed - 8/11/2012 14:45:24 - Evaluated as event OSX-Software_Update Host: 10.0.0.6
Aug 11, 2012 14:45:24 CDT	Software_Installed - 8/11/2012 14:45:24 - Evaluated as event OSX-Software_Update Host: 10.0.0.6

File and Directory Change Event Details

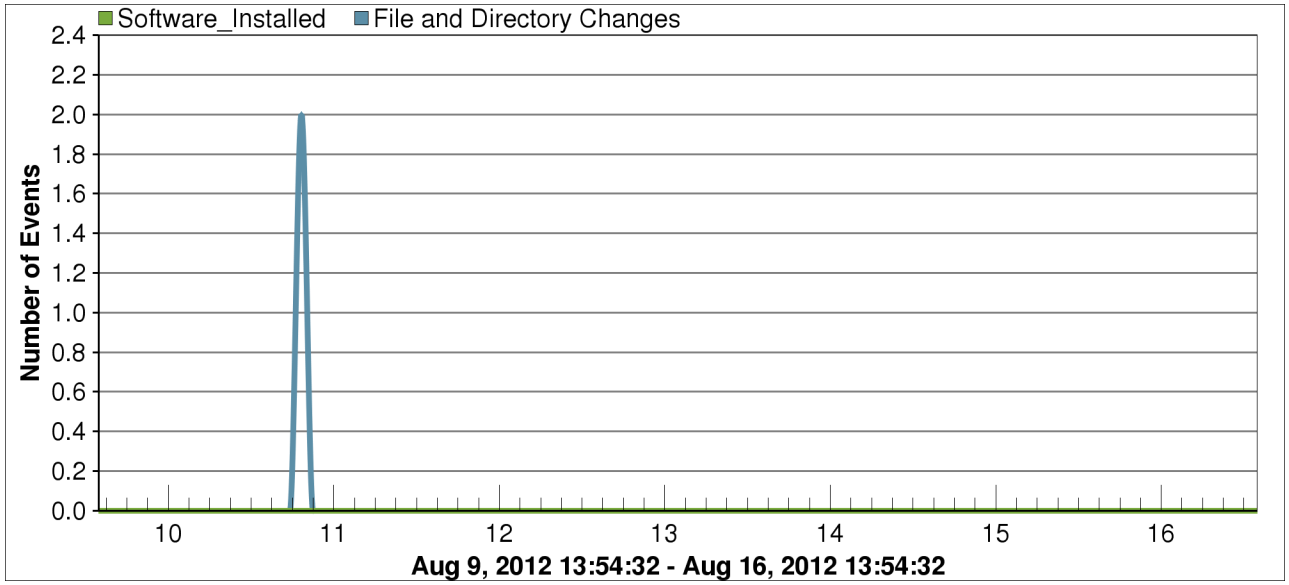
Time	Message
Aug 11, 2012 15:04:42 CDT	New file /var/db/receipts/com.apple.pkg.Safari6Lion.bom was added to monitored directory.
Aug 11, 2012 15:04:42 CDT	New file /var/db/receipts/com.apple.pkg.Safari6Lion.plist was added to monitored directory.
Aug 14, 2012 18:09:15 CDT	File /usr/bin/php-config has been modified. Its MD5 checksum changed from 010cdbe7290b7338450a1de85ea95eae to 4c3492f9cac5461696a8111bfbc160bc.

Time	Message
Aug 14, 2012 18:09:15 CDT	File /usr/lib/libssl.0.9.7.dylib has been modified. Its MD5 checksum changed from 58519be82d8226b47b03cf19e14e3267 to a1d66f7dd228f11c0b1dba41f6af4fb2.

10.0.0.7

Repository: Credentialed
DNS Name: MM2005.local
Vulnerabilities: Critical: 3, High: 9, Medium: 4, Low: 0, Info: 27
Last Scan: Aug 16, 2012 @ 1:23PM

Host Events



Details (Past 7 Days)

Software Installed Event Details

File and Directory Change Event Details

Time	Message
Aug 10, 2012 18:30:23 CDT	File /opt/lce_client/lce_client.conf has been modified. Its MD5 checksum changed from d8a152ce5fabed90b4de329065496b3c to 1cf29f1c7f95f8b39b1b01809202ecf1. Its permissions changed from 0644 to 0666.
Aug 10, 2012 18:30:23 CDT	File /etc/syslog.conf has been modified. Its MD5 checksum changed from de5fb242dd376a6634f5518f2a64c304 to 2fc89745d379e1638c18ae0e1cf87b20.