How Dtex Augments Log File Data and SIEM

The anonymized metadata in Dtex is both simpler and much more accurate than endpoint logs typically collected in a SIEM.

As you'll see from the common example in this presentation, Dtex provides simple, clear visibility of end-point activity unmatched by log files.

This presentation covers the following example:

7:54 AM
User creates folder, aggregates sensitive files

7:56 AM
User adds files to encrypted .rar archive

7:57 AM
User re-names file with .jpg extension to cover tracks

7:58 AM
User tries to use SCP to transfer file, but transfer fails

8:00 AM
User re-searches, downloads and installs Dropbox

8:02 AM
User copies file to Dropbox folder, file leaves

Volume of Records

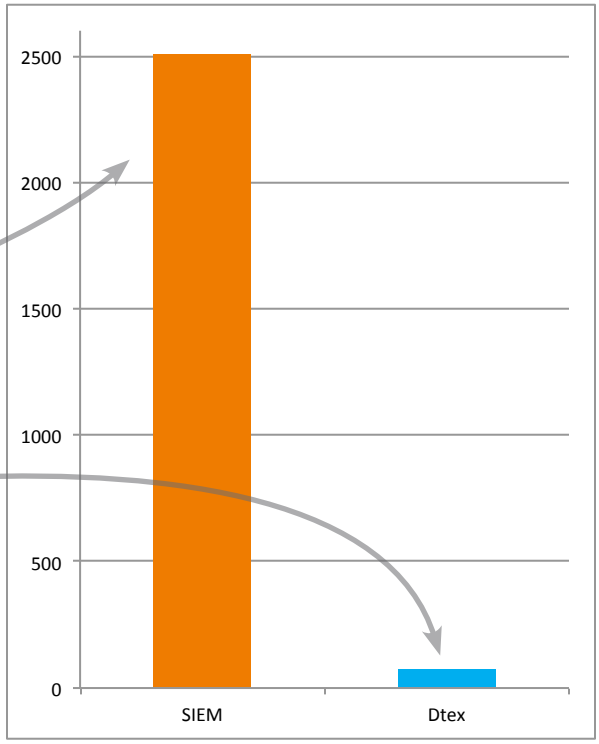
During this eight minute span:

- Windows Security Event Log (set to verbose logging):

  2,506 events

- Dtex (default configuration):

  Only 75 events



Quantity does not necessarily mean quality.

© Dtex Systems Group of Companies 2015

User Preparing to Steal Data

Dtex clearly shows the user consolidating files to a single folder.

Time	Activity	Details
3/2/15 7:54 AM	File Rename	New folder
3/2/15 7:55 AM	File Copy	\\psf\Home\Documents\Sensitive\Technical Overview - Windows MicroAgent.indd --> \\psf\Home\Desktop\Backup\Technical Overview - Windows MicroAgent.indd (Bytes: 5246976)
3/2/15 7:55 AM	File Copy	\\psf\Home\Documents\Sensitive\What Insiders Do.pdf --> \\psf\Home\Desktop\Backup\What Insiders Do.pdf (Bytes: 161919)
3/2/15 7:55 AM	File Copy	\\psf\Home\Documents\Sensitive\Technical Overview - Windows MicroAgent.pdf --> \\psf\Home\Desktop\Backup\Technical Overview - Windows MicroAgent.pdf (Bytes: 346856)
3/2/15 7:56 AM	File Copy	\\psf\Home\Documents\Sensitive\Log Files and the Insider Threat.pdf --> \\psf\Home\Desktop\Backup\Log Files and the Insider Threat.pdf (Bytes: 278541)

Despite capturing 149 records in Windows Event Log, none of them copying files from “Sensitive” to a new folder on their endpoint.

Dtex also clearly shows the user compressing, encrypting, and changing the name of the file in question to cover their tracks.

B	C	D
Time	Activity	Details
3/2/15 7:56 AM	Application Executed	WinRAR.exe
3/2/15 7:56 AM	Window Accessed	Archive name and parameters
3/2/15 7:56 AM	Window Accessed	Archiving with password
3/2/15 7:56 AM	Application Executed	dllhost.exe
3/2/15 7:56 AM	Application Executed	dllhost.exe
3/2/15 7:56 AM	File Rename	\\psf\Home\Desktop\\Backup.rar --> Mothers Blueberry Muffin Recipe.jpg.rar
3/2/15 7:57 AM	Application Executed	OpenWith.exe
3/2/15 7:57 AM	Application Executed	dllhost.exe
3/2/15 7:57 AM	Window Accessed	This PC
3/2/15 7:57 AM	Application Executed	dllhost.exe
3/2/15 7:57 AM	Application Executed	dllhost.exe
3/2/15 7:57 AM	File Rename	\\psf\Home\Desktop\\Mothers Blueberry Muffin Recipe.jpg.rar --> Mothers Blueberry Muffin Recipe.jpg

Windows Event Viewer only shows that WinRAR.exe was run, but not the actions taken by the user.

```
Process Information:
 New Process ID:  0x858
 New Process Name: C:\Program Files\WinRAR\WinRAR.exe
 Token Elevation Type: TokenElevationTypeLimited (3)
 Creator Process ID: 0x588
 Process Command Line:

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.
```

© Dtex Systems Group of Companies 2015

Exfiltrating the Data

Both Dtex and Windows Event Log files show that the user ran a command in Command Prompt in a blocked attempt to use WinSCP to move the data off-site. They also both clearly show that the user was running the Command Prompt as an Administrator, with elevated privileges.

Dtex:

Time	Activity	Details
3/2/15 7:57 AM	Window Accessed	Administrator: C:\Windows\System32\cmd.exe
3/2/15 7:58 AM	Window Accessed	Administrator: C:\Windows\System32\cmd.exe - dir

Windows Event:

Process Information:
New Process ID: 0x13d8
New Process Name: C:\Windows\System32\cmd.exe
Token Elevation Type: TokenElevationTypeFull (2)
Creator Process ID: 0x588
Process Command Line:

Both Dtex and Windows Event Log files show the Dropbox application running.

However, Windows Event Log only shows the Dropbox application being executed:

Process Information:
New Process ID: 0xcb0
New Process Name: \Device\Mup\psf\Home\Downloads\DropboxInstaller.exe
Token Elevation Type: TokenElevationTypeLimited (3)
Creator Process ID: 0x2ac
Process Command Line:

Dtex shows the complete user context, from web activity to download to installation:

Time	Activity	Details
3/2/15 8:00 AM	Application Executed	chrome.exe
3/2/15 8:00 AM	Window Accessed	New Tab - Google Chrome
3/2/15 8:00 AM	Window Accessed	https://www.dropbox.com - Google Chrome
3/2/15 8:00 AM	Window Accessed	Dropbox - Google Chrome
3/2/15 8:00 AM	File Create	explorer.exe --> BBi9cpu[1].jpg
3/2/15 8:00 AM	File Create	DropboxInstaller.exe --> WSH3XCIX.txt
3/2/15 8:00 AM	File Create	DropboxInstaller.exe --> ZNP1VPJH.txt
3/2/15 8:00 AM	File Create	DropboxInstaller.exe --> Z61MSZ1G.txt
3/2/15 8:00 AM	File Create	DropboxInstaller.exe --> XPE7PQ1S.txt
3/2/15 8:00 AM	Window Accessed	Dropbox Installer
3/2/15 8:00 AM	Application Executed	ThumbnailExtractionHost.exe
3/2/15 8:00 AM	Application Executed	DropboxData.exe
3/2/15 8:00 AM	Window Accessed	Dropbox Installer

And Dtex shows the smoking gun - the user copying the file to the Dropbox folder that syncs with the Dropbox cloud service.

Time	Activity	Details
3/2/15 8:02 AM	File Copy	\\psf\Home\Desktop\Mothers Blueberry Muffin Recipe.jpg --> C:\Users\user\Dropbox\Mothers Blueberry Muffin Recipe.jpg

This is one of scores of examples of insider threat activity that's impossible to catch in companies that rely solely on log files gathered by SIEM systems.

© Dtex Systems Group of Companies 2015