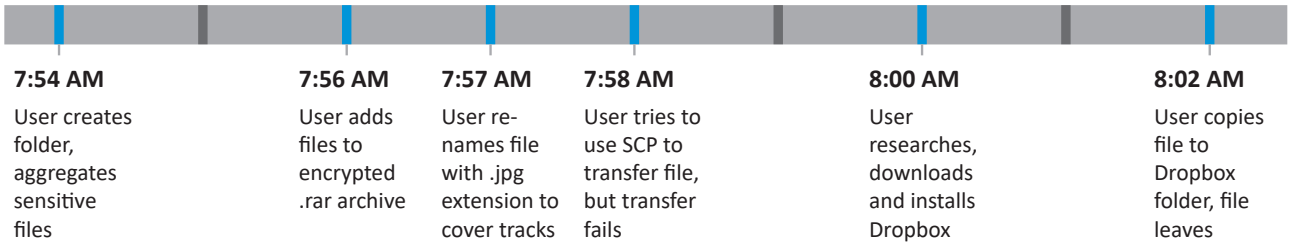
How DTEX Compliments SIEM Systems

DTEX integrates seamlessly with Security Incident and Event Management (SIEM) systems to provide actionable alerts and visibility into user threats.

The DTEX Workforce Cyber Intelligence Platform complements SIEM systems to produce a consolidated and transparent view of user activity. SIEM systems consolidate a substantial volume of data from logs - which can result in an overwhelming number of events. By contrast, DTEX uses analytics to pinpoint the most relevant events. In addition, SIEM systems - while sophisticated in their capability to collect, integrate and analyze data from multiple disparate sources - do not necessarily have visibility into user activities on endpoint devices.

This scenario illustrates how DTEX workforce cyber intelligence provides a simple and clear view of endpoint activity. In this case a short sequence of user activities representing high-risk behavior creates several thousand windows events that can be very difficult to review and interpret. By contrast, DTEX user behavior intelligence produces less than 100 events.



Volume of Records

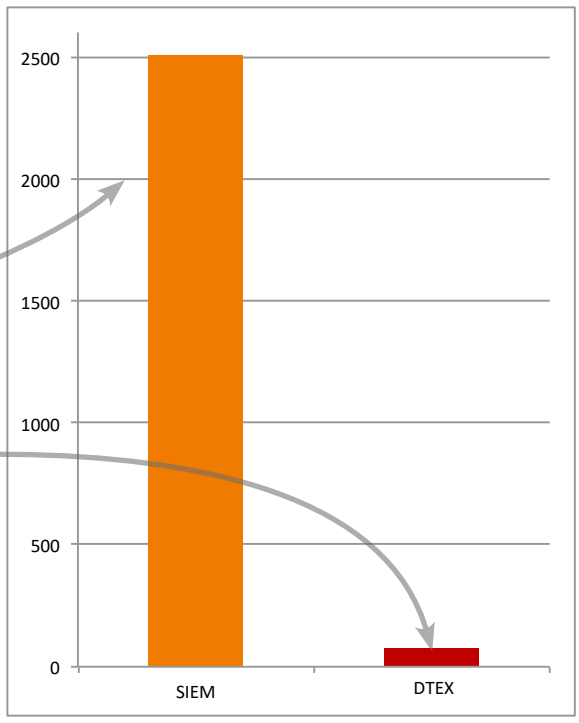
During this eight minute span:

Windows Security Event Log (set to verbose logging):

2,506 events

DTEX's Endpoint Security Analytics:

Only 75 events



Stage 1: User Preparing to Steal Data

Continuing this scenario, DTEX clearly shows the user consolidating files into 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)

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.
```

Stage 2: User Exfiltrating the Data

Then, this user attempted to exfiltrate 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, on the other hand, shows the complete user context. You can clearly see every event leading up to the data theft, from web activity to download to Dropbox 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

Most importantly, DTEX shows the smoking gun. Here, you see 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

While the Windows Event Log was able to log some events in this very common data exfiltration scenario, it didn't provide the visibility that analysts need to understand the full scenario - and worse, those few relevant events were buried within thousands of logs. With DTEX, you get full user visibility and advanced analytics that cut through the noise, ensuring that you see the most relevant threats in your organization. Using the DTEX User Behavior Intelligence Platform alongside your SIEM solution will give you a greater level of intelligence into your organization than ever before.

See How DTEX Fits in Your Organization

A DTEX Insider Threat Assessment can show you what your SIEM is missing. During your assessment, DTEX's analysts will work with you to show you how DTEX InTERCEPT catches the risks in your organization - and will sum up your threats in one complete report.
Contact your sales representative or info@dtexsystems.com to get started.