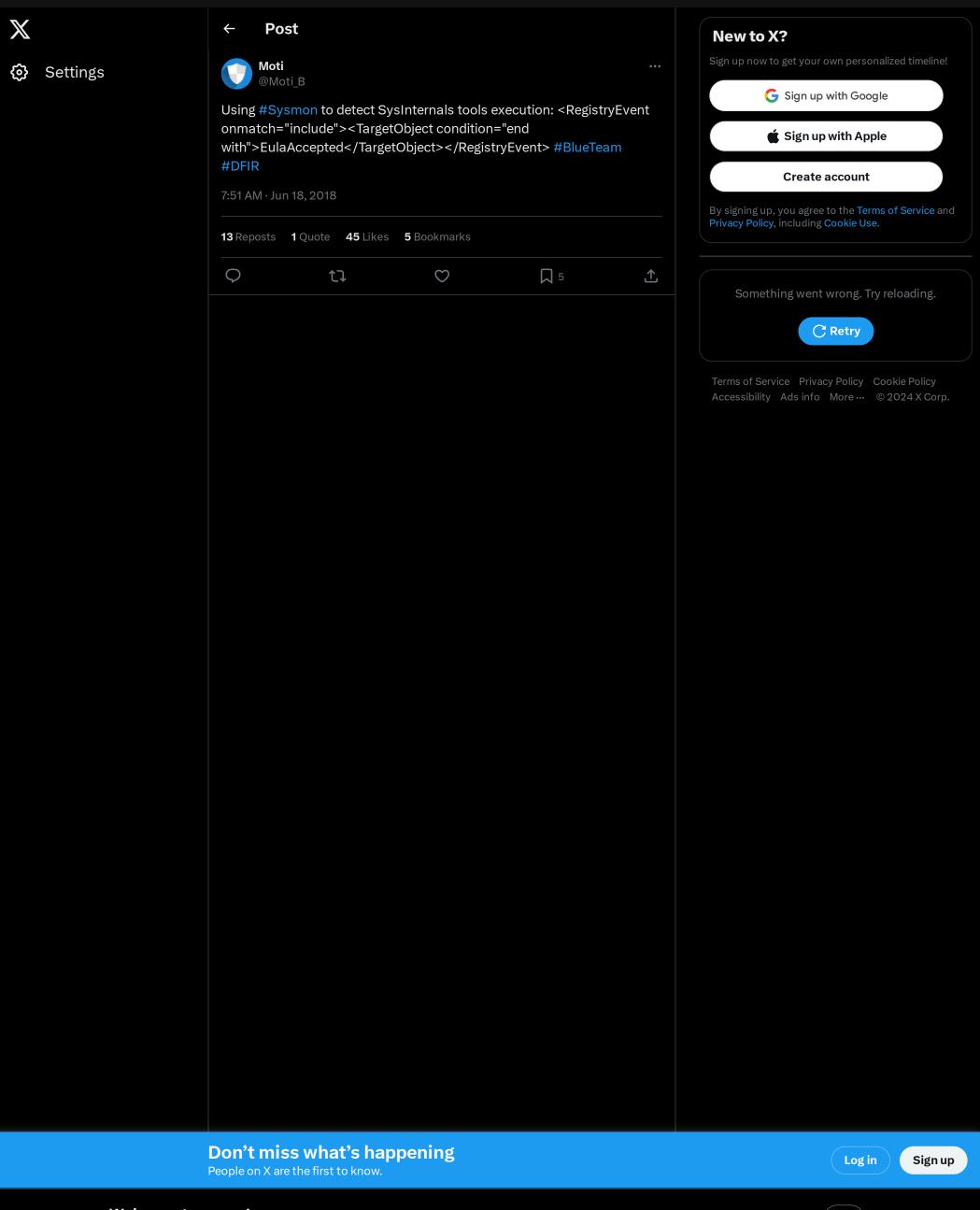
Moti on X: "Using #Sysmon to detect SysInternals tools execution: <RegistryEvent onmatch="include"><TargetObject condition="end with">EulaAccepted</TargetObject></RegistryEvent> #BlueTeam #DFIR" / X - 02/11/2024 17:01
https://x.com/Moti_B/status/1008587936735035392



Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same. For more details, see our Privacy Policy: https://x.com/en/privacy

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. Show more about your choices.

Accept all cookies

Refuse non-essential cookies