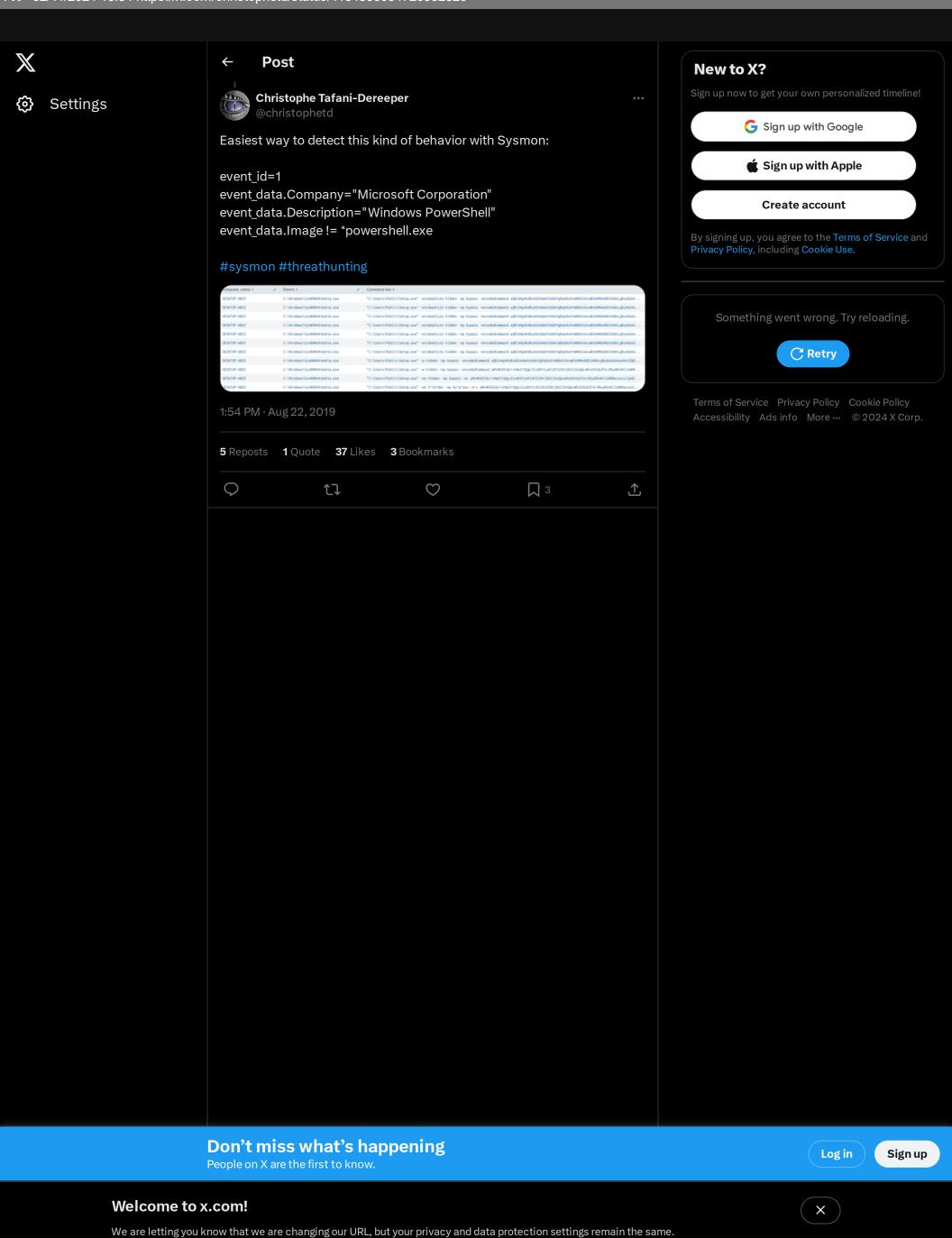
Christophe Tafani-Dereeper on X: "Easiest way to detect this kind of behavior with Sysmon: event_id=1 event_data.Company="Microsoft Corporation" event_data.Description="Windows PowerShell" event_data.Image != *powershell.exe #sysmon #threathunting https://t.co/tl9cOTE87k" / X - 02/11/2024 16:34 https://x.com/christophetd/status/1164506034720952320



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.

For more details, see our Privacy Policy: https://x.com/en/privacy

Accept all cookies

Refuse non-essential cookies