* Event ID 4648, A logon was attempted using explicit credentials.

A user connects to a server or runs a program locally using alternate credentials. Meaning that if User1 is logged in, they’ve run a program locally with a separate set of credentials, likely one with administrative privileges. This Event ID corresponds with many Techniques from METRE’s ATT&CK Matrix such as:

Abuse Elevation Control Mechanism

Bypass User Account Control

* Event ID 4625, An account failed to log on.

This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account. This is extremely useful to watch for because one of the key things to pay attention to is multiple occurrences of this event; which could indicate a Brute Force attempt.  
  
Brute Force:

Password Guessing

Password Cracking

* Event ID 4697, A service was installed in the system.

A new service was installed by the user indicated in the subject. Subject often identifies the local system (SYSTEM) for services installed as part of native Windows components and therefore you can't determine who actually initiated the installation. This is a key change control event as new services are significant extensions of the software running on a server and the roles it performs. This event ID relates to but is not limited to:

Installer Packages

Server Software Component