Event Analysis: Remote Logon Activity

These analysed events were recorded when remote SSH login attempts either succeeded (ID 4264) or failed (ID 4265). Important information included:

- For failed logins, all the events were of logon type 8: network cleartext (unencrypted credentials)
- For successful logins, the events appeared in groups of two, rarely three. These were of Logon Type 3 paired with 8, which makes sense for a default SSH configuration without any security measures as this was what was used for testing. There were some outliers where they were two Logon Type 3 events paired. This was unexpected considering those used the exact same security configuration as the logon attempts paired with Logon Type 8

This has unfortunate implications for the implementation of the unsuccessful remote login use case. If a secure SSH configuration is used, there does not seem to be a Logon Type that logs encrypted credentials, so these events would stop appearing.

For a successful login, if it was unexpected, the logon ID field could be used for correlation to ascertain the actions performed in the session.

20:40:14.7...	W11-VM_agent	Successful Remote Login D...	13	100116	8
20:40:12.3...	W11-VM_agent	Successful Remote Login D...	13	100116	3
20:40:02.7...	W11-VM_agent	Successful Remote Login D...	13	100116	3
18:42:21.3...	W11-VM_agent	Successful Remote Login D...	13	100116	8
18:42:19.3...	W11-VM_agent	Successful Remote Login D...	13	100116	3

Figure 1: 2 Example Event Bursts for Successful Remote Login Attempts