Ransomware Detection

PLATFORM FEATURE UPDATE

While various ransomware attacks use different methods and techniques, at the core, the attack is carried out by encrypting files across a victim's network. In doing so, this process triggers a number of file access events: Write/WriteAttribute (Windows Event ID 4663) and Delete (Windows Event ID 4660).

Adlumin's new **Ransomware Detection Model** monitors the volume of these three events independently of each other per user across the entire network, looking for anomalous spikes in activity during a specific time window using historical data as a benchmark. If the amount of activity (either write or deletion) exceeds a specific threshold relative to the rest of the activity on the network, a detection will be sent for investigation.

In addition to checking the total volume of files accessed, the model also checks the distribution of objects modified across the network. If the majority of activity is focused in a single directory, which could be associated with software installation or updates, the model will not raise a detection. However, if the spike in activity is spread across multiple subdirectories, indicative of system-wide activity, the model will raise a detection.