Lateral Movement Detections (pt. 1)

PLATFORM FEATURE UPDATE

When an attacker moves laterally on your network, they are likely to leave a trace of access events. The lateral movement model learns the normal patterns of access on your network and alerts you when a privileged user's behavior deviates significantly from that baseline. Machines associated with anomalous behavior are flagged, and the associated user's behavior over the course of the day is summarized in the detection to help security analysts further investigate.

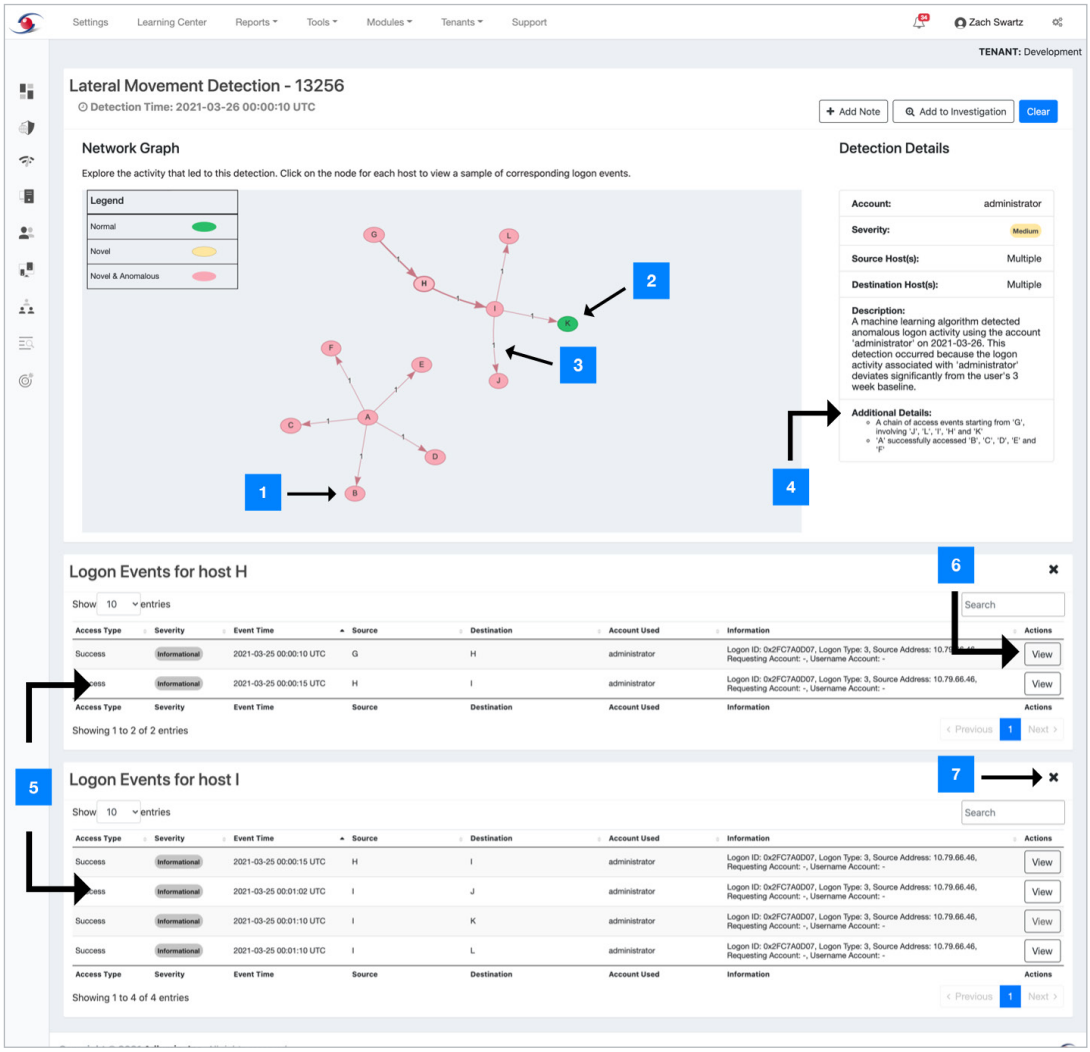
Some important things to note are:

- This algorithm only monitors accounts with privileged access.
- Since a lateral attack is likely to involve machines that are rarely accessed by a given user, a detection is only triggered if the anomalous pattern of behavior involves rare or 'novel' machines. The purpose of this is to avoid false positives.
- Anomaly scores are assigned to machines individually. The severity of the detection is associated with the highest anomaly score.

continues on next pg. »

Lateral Movement Detections (pt. 2)

PLATFORM FEATURE UPDATE



Per the image above, specific features of the page include:

1. Machines are colored red if they are both novel and involved in a suspicious pattern of behavior.
2. Machines are colored green if they are present in the user's history.
3. This connection represents a single access from machine 'I' to machine 'J'.
4. Look for descriptions of distinct patterns.
5. Clicking on a graph node will spawn a table of access events.
6. Click to view full access event.
7. Click to remove table from view.