

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

The screenshot displays the 'Lateral Movement Detection - 13256' interface. At the top, navigation tabs include Settings, Learning Center, Reports, Tools, Modules, Tenants, and Support. The user 'Zach Swartz' is logged in. The main content area is divided into three sections:

- Network Graph:** A central diagram showing nodes (A-L) and connections. A legend indicates node colors: Normal (green), Novel (yellow), and Novel & Anomalous (red). Nodes G, H, I, J, and L are red, while node A is green. Blue callouts 1-4 point to specific nodes and connections.
- Detection Details:** A sidebar on the right providing metadata: Account (administrator), Severity (Medium), Source Host(s) (Multiple), and Destination Host(s) (Multiple). A description explains the machine learning algorithm's findings. An 'Additional Details' section lists a chain of events starting from 'G'.
- Logon Events for host H:** A table showing two entries. The first entry shows a successful login from source 'G' to destination 'H'. The second entry shows a successful login from source 'H' to destination 'I'. A blue callout 6 points to the 'View' button for the second entry.
- Logon Events for host I:** A table showing four entries, each representing a successful login from source 'I' to destinations 'J', 'K', and 'L'. A blue callout 5 points to the first entry, and a blue callout 7 points to the 'View' button for the last entry.

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.