

Malicious PowerShell Detections

PLATFORM FEATURE UPDATE

PowerShell is a trusted management tool for system administrators that is also frequently used as an attack vector. The Malicious PowerShell Detection model utilizes a large dataset of legitimate PowerShell executions to detect string patterns associated with normal operations. PowerShell executions that break these patterns are flagged as anomalous and the behavior is summarized to help security analysts determine its significance.

Some important things to note are:

- Anomalous PowerShell executions are grouped together in one detection if they have similar signatures.
- Any execution containing 'PowerShell' in the command-line is a candidate for this detection.
- This model executes daily and produces detections for the previous day.

The screenshot displays the Adlumin interface for a specific detection. At the top, there is a navigation bar with 'Settings', 'Learning Center', 'Reports', 'Tools', 'Modules', 'Tenants', and 'Support'. The current tenant is 'TENANT: Demonstration Tenant'. The main heading is 'Process Execution Detection - 15819' with a sub-heading 'Detection Time: 2021-08-09 07:40:35 UTC'. There are three buttons: '+ Add Note', 'Add to Investigation', and 'Clear'. Below this is the 'Detection Details' section, which states: 'A machine learning algorithm has identified an anomalous set of process executions. Details: powershell.exe -download'. To the right of this text are three summary cards: 'Total Events' (5 Events Surrounding this Detection), 'First Occurrence' (2021-08-09 07:40:35 UTC), and 'Last Occurrence' (2021-08-09 07:41:15 UTC). The 'Event Timeline' section shows a horizontal timeline with five events: 'August 09 2021 @ 07:40:35 Process: ping.exe', 'August 09 2021 @ 07:40:45 Process: powershell.exe', 'August 09 2021 @ 07:40:55 Process: powershell.exe', 'August 09 2021 @ 07:41:05 Process: powershell.exe', and 'August 09 2021 @ 07:41:15 Process: wscript.exe'. The 'Surrounding Events' section at the bottom has a 'Show 10 entries' dropdown and a search box.