JULY 2021

Cisco Advanced Malware Protection (AMP) Support

PLATFORM FEATURE UPDATE

Adlumin has added support for Cisco Advanced Malware Protection (AMP); it is also referred to as Cisco Secure Endpoint. This new API integration allows you to bring all your AMP event logs into Adlumin for parsing and analysis. Enabling this new functionality is as simple as generating an API key through the AMP Console, and linking that key to Adlumin through the new Cisco AMP user interface. Once linked, Adlumin will continuously poll the AMP API servers for new events. Custom detections allow you to receive real-time alerts for AMP events that match specified criteria.

In the coming months, Cisco AMP support will be added to Adlumin's SOAR capabilities, allowing you to automatically disable devices through the AMP API if a threat is detected.

To support this upcoming feature, be sure to enable 'read and write access' when generating the AMP API key. You can access this functionality under ***Devices*** > ***Endpoint Security*** > ***Cisco AMP***.

For information on generating an AMP API key, visit:
https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/201121-Overview-of-the-Cisco-AMP-for-Endpoints.html#anc1