

Microsoft Defender Antivirus Scanning [SOAR Support]

PLATFORM FEATURE UPDATE

Adlumin users have the ability for Microsoft Defender Antivirus scanning in response to potential malware. The new feature automatically initiates a Microsoft Defender Antivirus scan in response to potential malware activity. The action will conduct a Windows Defender full-system scan with the intent of eliminating identified malware as well as additional malware activity yet to be identified.

You can access this new feature under *Tools > SOAR Support* in the top navigation bar.

The screenshot displays the Adlumin Security Orchestration Automation and Response (SOAR) interface. The top navigation bar includes 'Settings', 'Learning Center', 'Reports', 'Tools', 'Modules', 'Tenants', and 'Support'. The main content area is titled 'Security Orchestration Automation and Response (SOAR)' and features a sidebar with 'Automated Playbooks' and 'Manual Response'. The 'Manual Response' section lists five configuration options, each with a description and a green 'On' toggle switch:

- Response to a VPN client compromise.**
This configuration will automatically disable an account when an analytic algorithm determines there is an extremely high likelihood of VPN account compromise. For example, a successful login from a foreign country or impossible travel. For this feature to operate nominally you must have Adlumin clients deployed to your domain controllers, VPN authentication linked to Active Directory, and VPN session parsing must be operational.
- Response to an IIS/OWA compromise.**
This configuration will automatically disable an account when an analytic algorithm determines there is an extremely high likelihood of a compromise across IIS services. For example, a successful access event from a foreign country or impossible travel. For this feature to operate nominally you must have Adlumin clients deployed to your domain controllers and IIS logs ingesting into any miscellaneous device data port.
- Response to an O365/Azure compromise.**
This configuration will automatically disable an account when an analytic algorithm determines there is an extremely high likelihood of a compromise across O365/Azure services. For example, a successful access event from a foreign country or impossible travel. For this feature to operate nominally you must have Adlumin clients deployed to your domain controllers and be using the Office365/Azure portal API integration, not the cloud app security integration.
- Dark Net Exposure auto-password reset.**
This configuration will automatically force an account to reset their password at the next legitimate login when the account has been exposed in a dark net exposure breach. This configuration only applies to Critical and High severity events. For this feature to operate nominally you must have Adlumin clients deployed to your domain controllers and the dark net exposure module must be active.
- Defender Anti-Malware Scan in Response to Potential Malware.**
This configuration will automatically initiate a Windows Defender anti-malware scan in response to potential malware activity. This action will conduct a windows defender full system scan with the intent of eliminating identified malware as well as additional malware activity yet to be identified.

Copyright © 2021 Adlumin, Inc. All rights reserved.