

PRODUCT UPDATE 5.14.1.0 - OCTOBER 1, 2024

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 5.14.1.0 of the MA-SV platform.

Bug fixes

- Fixed an issue where testing queries returned "null" in results without indication of error.
- Fixed an issue where the AEDA landing page didn't indicate that monitors were broken.
- Fixed an issue where the Operation Status incorrectly stated that Remote Integration tests were failing.
- Fixed an issue where Jobs indefinitely stalled in between groups.
- Fixed an issue where the AEDA landing page was taking too long to update.
- Fixed an issue where the LoginUI.exe process took too long to restart when a Network Action was run with an interactive session using a Windows system as the source Actor.
- Fixed an issue where scheduled Jobs couldn't be edited.
- Fixed an issue where AWS MSI integrations were not showing the integration names in Suspicious Event.
- Fixed an issue where Protected Theater was unable to connect to a security center domain that is needed for Microsoft Defender for Endpoint functionality.
- Fixed an issue where the Job Action Result window wasn't displaying any data.
- Fixed an issue where filtered events weren't appearing for the Microsoft Azure Sentinel Integration.
- Fixed an issue where Jobs couldn't be scheduled at specific times.
- Fixed an issue where Job Results pages weren't showing events from Splunk.
- Fixed an issue where the support portal link was incorrect.
- Fixed an issue that prevented Actions from being run.

Known issues

- When you add the first MSI integration on a Remote Integrations Actor, the integration does not get detected. To fix this, reboot the Actor after the first MSI integration is selected for that Actor.
- Local Event Filtering works as expected but is limited to Match Action, Match Integration, and Match Events (when the latter involves Raw Events). If a rule has a Match Event condition for any field other than Raw Event, the rule does not apply to Local Events. It only applies to events from standard local integrations in Security Validation.