Mandiant

PRODUCT UPDATE 5.12.0.0 - OCTOBER 12, 2023

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 5.12.0.0 of the MA-SV platform.

General Enhancements

- New Integrations Service Preview for streamlining local and remote integrations setup and configuration. Customers are strongly encouraged to use the new Preview Integrations as they are updated most frequently, including nightly builds as part of our **security patches** (https://docs.mandiant.com/home/msv-security-patch-downloads). For more information, see the **Preview Integrations** (https://docs.mandiant.com/home/msv-preview-integrations) documentation.
- Added support for **MITRE ATT&CK version 13.1** (https://attack.mitre.org/versions/v13/)
- Extended Pipelines functionality to support delivering job results to one or more Webhook destinations, enabling easier integration with data lakes. For more information, see the **Pipelines** (https://docs.mandiant.com/home/msv-pipelines) documentation.
- Ransomware Defense Validation (RDV) is Generally Available to MA-SV customers as of this release. For more information, see **Get Started with Ransomware Defense in Security Validation** (https://docs.mandiant.com/home/msv-get-started-rdv).
  Features include:
  - RDV content that repurposes actual ransomware and controls it so it can be executed safely. This content is available with an RDV license.
  - First-time setup for configuring Windows Actors and schedules specific to running RDV content.
  - Reporting that includes quantifiable data to demonstrate your security controls' ability to withstand the most likely ransomware attacks
  - A dashboard that provides an overview of RDV-related data in your organization
  - NOTE: Previously, any interruption of the RDV testing process was categorized as a blocked outcome, which is inaccurate. From 5.12.0.0 onward, an RDV payload that cannot be initiated is tagged with an errored state instead.

- Cloud Validation Module (CVM) is Generally Available to MA-SV customers as of this release. For more information, see the **Cloud Validation Module** (https://docs.mandiant.com/home/test-cloud-controls) documentation. Features include:
  - Cloud integrations for Google Cloud, Azure, and AWS
  - Content creation
  - Behavior Research Team (BRT) curated content is available with a CVM license

- Content Library Enhancements including changes to viewing and filtering Actions, Evaluations, and Sequences, including the following:
  - Changed the default home page to the Sequence Library, sorted by Last Added
  - Improved Filtering by Last Run job status and enhanced Filter Dimensions
  - Highlights for content updates, including the "New" status indicator
  - Enhanced sorting options
  - Cleaner, tiled Actions list
  - Last Ran date and Status
  - Paginated content list loads in seconds as opposed to minutes
  - Enhanced Preview panel with links to Jobs
  - **Actions, Sequences, and Evaluations** (https://docs.mandiant.com/home/msv-running-security-content-working-with-jobs) documentation updated to reflect the Content Library Enhancements

Bug Fixes

- Addressed an issue where Cloudflare returned a 521 HTTP response to the MA-SV Director
- Fixed an issue where Operational Status emails were not being generated and sent

- Fixed a Content Library issue where sort by "Name" with ascending order was not displaying results in the proper order
- Fixed a Content Library issue where the last Action description was being truncated
- Fixed an issue where deleting an action could result in 400-series error
- Fixed an issue where the Suspicious Events filter was not exporting events correctly
- Fixed an issue where Protected Theater map and integrations displayed conflicting data
- Fixed an issue where Protected Theater upgrades stopped with message "Waiting for Protected Actor to come online" and the Protected Actor was not reachable
- Fixed an issue where the Action Preview was failing to display
- Fixed an issue in the Content Library where the "New evaluation from selected" or "New sequences from selected" options were not functioning
- Fixed an issue where the Actions queue was displaying the incorrect total number of Actions
- Fixed an issue where Jobs were sometimes matching to the incorrect Security Technology on the endpoint
- Fixed an issue where Network actions would unexpectedly error out with an apparent need for HTTP credentials even though there was not any device expecting the credentials
- Fixed an issue where the Pull Actor service would eventually stop processing incoming requests from Network and Endpoint Actors
- Fixed an issue where the Security Technology values did not always populate when creating AEDA monitor from existing Jobs
- Fixed an issue where modifying a Scheduled or Repeating Job would clear the "Target Domain" field
- Fixed an issue where email profiles would be deleted when no Actors were assigned

Known Issues

- Local Event Filtering works as expected but is limited to Match Action, Match Integration, and Match Events (when the latter involve 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 MSV.
- Preview Remote Integrations are not yet supported for installer-based Actors. These integrations only work for appliance-based Actors at this time. Support is coming for installer-based Actors prior to full GA of the new Integrations.