Mandiant

PRODUCT UPDATE 5.14.0.0 - JUNE 6, 2024

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 5.14.0.0 of the MSV platform.

General Enhancements

- Note that the **minimum hardware and OS requirements** **(https://docs.mandiant.com/home/msv-network-actor-requirements)** have changed for MSV Actor Appliances that are upgraded to 4.14. The requirements are as follows:
  - CPU: 64-bit x86 with at least 2 cores
  - Minimum RAM: 2 GB
  - Minimum Disk Space: 60 GB (up from 20 GB)
  - Network Interfaces Required: 2
  - Static, Routable IPs: 1
  - Base Operating System for new installations: Rocky Linux 8 (formerly CentOS 7)
  - Moving forward, changes to Actor Networking (IP Address, Netmask, Gateway, DNS, and so on) are done using the `vsetnet` CLI tool on the Actor OVA. SSH access is required to the Actor. The `vsetnet` tool is also used for selecting Interface Assignments (management, simulation, monitor). As of 5.14.0.0, this functionality is no longer available in the Director web interface.
  - Other Changes
    - Added the ability to define two DNS servers per Actor.
    - PX Proxy is used instead of CNTLM on Director for NTLM connections.
    - SSL Protocol explicitly only allows TLSv1.2 and Cipher Suites.
- Performance and stability improvements for the following:
  - Audit Log
  - Job Status page
  - Suspicious Events page

Bug Fixes

- Fixed an issue where email queries from a Splunk MSI integration resulted in an error 422 when using invalid email format.
- Fixed an issue where Email Threater account verification was failing with no visible error.
- Fixed an issue where the Actor would attempt to write to the system-wide Kerberos configuration.
- Fixed an issue where events weren't dropped or suppressed from the Jobs view.
- Fixed an issue where suspicious events were not being deleted.
- Fixed an issue where a QRadar integration was not returning events.
- Fixed an issue where MA-SV was unable to associate Threat Intel information to Threat Actors when a Threat Intel provider was already integrated.
- Fixed a cosmetic issue where a newly-added Protected Theater showed as a Protected Actor in the web interface.
- Fixed an issue where files could not be added when editing an Action.
- Fixed an issue where a Splunk ES Cloud Classic Direct Integration was not pulling notables.
- Fixed an issue where validate Actor version tests were disabled but emails for tests continued to be sent.
- Fixed an issue where Events weren't opening on the Job Status page.
- Fixed a cosmetic issue where a Rocky Linux image incorrectly appeared as CentOS in the web interface.
- Fixed an issue where the regex for Splunk was unable to post "Search Replacements."
- Fixed an issue where the Test button was grayed out on a QRadar integration.
- Fixed an issue where blocked Protected Actions were not populating detection events.

Known Issues

- After migrating Actors to the Rocky Linux 8-based VM, Remote Integrations may fail. **Use the steps in this**

document **(https://docs.mandiant.com/home/msv-upgrade-rocky-linux#workaround-remote-integrations-fail-to-report-events)** as a workaround.

- 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.
- The Network Map is zoomed out and appears with a narrow height, but still functions correctly. Users can still zoom in and out, move the map around, and select Actors as needed.
- 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.