Mandiant

PRODUCT UPDATE 4.8.2.0 - MARCH 21, 2022

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 4.8.2.0 of the platform. This release adds several new and enhanced capabilities to the Validation Platform, including ***Report Builder enhancements, the ability to re-attach Actors, user experience improvements, and bug fixes.***

Important Installation Notes

- **Minimum Director Version.** Director version 4.6.3.0 or higher is required to upgrade to version 4.8.2.0.
- **Actor Compatibility**. Actors must be upgraded to at least version 4.6.0.0 before updating Director to 4.8.2.0.

New Features and Updates

- **Content Service usability Improvements.** You can configure the content service to only download and not apply the new content packs, with a visual progress indicator displaying for downloads. There is also improved information around any errors that occur. The content service runs every hour, but you can use the **restart** button found in **Support Settings** to have it run immediately.
    - **Reminder**. Directors with licenses issued after January 1, 2022 are configured to automatically download and apply newly published Mandiant content. All others must enable the content service.
- **Report Builder Updates**. You can now select the time scale for time series bar charts. You can also exclude columns from the security technology bar charts. When exporting PDFs, you have an option to download just the charts. Admin users can now update reports created by other users.
- **Actor Reattachment.** You can reuse an Actor definition using the reattach option in **Actor Settings**. To do this, the new Actor must have the same functionality and you must run vreset. This allows your existing Monitors to continue using the Actor. The re-attached Actor information includes a section for the original IP addresses used, allowing you to easily trace the Actor.

General Improvements

- Port Scan Job Action Results have been improved:
    - No longer displaying pass / fail information
    - When there are multiple Port scan Actions included in Jobs, they are called out separately in the status graphic and not included in pass / fail calculations.
- There are new Protected Theater Settings that automatically create the necessary DNS and Communication rules when you run Protected Actions while connected to a non-local Director.
- You can cancel a single Job Actions from the Job Queue page.
- Several UI Improvements were made to the Operational Status page.
- The Product telemetry collection setting is now enabled by default.
- To assist with troubleshooting, Actor upgrade failure information is available to the Director and included in the logs.
- Action Scripts are displayed using standard script color schemes when viewing the script in Action preview or Job Results.
- In-platform documentation available when creating Host CLI Actions documents that success_match, blocked_match, and error_match are case-insensitive.
- The Elastic Integration was updated to include a Sub-cluster prefix input field.
- Improve the job_errors.yml file to capture all known use cases from actor failures.

Bug Fixes

Issue key	Summary

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

MSV-2265	Monitor: TCP Scan monitors construction doesn't consume open/closed results
MSV-2397	Remove additional wait time after session times out
MSV-2747	Monitor: Error while sending Monitor Notifications
MSV-2790	Director Over Utilization of Resources
MSV-2879	Sleep actions are counted as "Not Blocked" in custom reports
MSV-3029	Proxy using Kerberos authentication on Windows Actors
MSV-3187	Splunk integration failed to fire on multiple Actions in a Job
MSV-3227	AD Settings for User Changes When Using Group Mapping Functionality
MSV-3281	McAfee ePolicy Orchestrator Integration not collecting events - warn "valid so we're not adding a JaEvent for it on Job"
MSV-3284	Exception during port scan actions
MSV-3286	Data from Anomali TAAM feed missing/incomplete
MSV-3298	Detecting technologies not displayed correctly in Report Builder
MSV-3316	Cancellation of Protected Action while in sectech delay period does not immediately restore snapshot
MSV-3333	Host CLI Actions fail when Defender is detected but its Event log is not present
MSV-3339	Fix missing object reference on failed connection to perform Actor upgrade
MSV-3342	Crowdstrike integration default discovery field has changed for Splunk and QRadar
MSV-3357	Content Application: Application process is running for > 24 hours

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

MSV-3361	DNS Actions don't count as blocked even though IP addresses provided in BlackHole IP Addresses.
MSV-3364	Cortex XDR sectech definition not working
MSV-3414	UI/UX: Integration status unknown
MSV-3435	Jobs using web proxy change destination address to web proxy IP
MSV-3443	Incorrect Job Status: Action was not blocked however action status reflected "Errored" message.
MSV-3456	Suppressed events from blocking technologies are being counted in ReportBuilder Widgets
MSV-3521	Remote integrations and NX
MSV-3532	Small VAS Installation hangs
MSV-3553	Environment map rendering issues in Edge and Chrome
MSV-3560	Actors failing to update from 4.6.3.0 to 4.7.0.2
MSV-3561	SAML fails in 4.8.1 with Ping SSO and latest browser
MSV-3595	"Updated integrations package on actor" should not appear for TIP integration
MSV-3644	Not able to register Windows actors 4.8.1.0
MSV-3650	Heat map removed from access in MSV customers after upgrading to 4.8.1
MSV-3672	Sleep Actions within a group of DNS Actions breaks the start / end time which breaks event matching

Appliance OS Security Update

Mandiant uses **Red Hat's security ratings** **(https://access.redhat.com/security/updates/classification)**to determine the criticality of vulnerabilities identified and resolved. This rating system is a combination of a four- point scale and the Common Vulnerability Scoring System (CVSS) base scores.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Mandiant

The Mandiant Advantage Security Validation Product team would like to announce the availability of a security update for the platform. This security update applies to Directors, Actors, and Protected Theaters that are virtual appliances. The criticality of the vulnerabilities resolved are listed below.

	Director	Actor	Protected Theater
Critical	0	0	0
High	2	2	3
Medium	1	1	1
Low	2	0	0

Details for the High severity vulnerabilities against the Director are as follows:

- CentOS 7 : cyrus-sasl (CESA-2022:0666): The remote CentOS Linux host is missing a security update. (CVE-2022-24407)
- CentOS 7 : kernel (CESA-2022:0620): The remote CentOS Linux host is missing one or more security updates. (CVE-2021-3752)

Details for the High severity vulnerabilities against the Actor are as follows:

- CentOS 7 : cyrus-sasl (CESA-2022:0666): The remote CentOS Linux host is missing a security update. (CVE-2022-24407)
- CentOS 7 : kernel (CESA-2022:0620): The remote CentOS Linux host is missing one or more security updates. (CVE-2021-3752)

Details for the High severity vulnerabilities against the Protected Theater are as follows:

- CentOS 7 : cyrus-sasl (CESA-2022:0666): The remote CentOS Linux host is missing a security update. (CVE-2022-24407)
- CentOS 7 : kernel (CESA-2022:0620): The remote CentOS Linux host is missing one or more security updates. (CVE-2021-3752)
- CentOS 7 : firefox (CESA-2022:0514): The remote CentOS Linux host is missing one or more security updates. (CVE-2022-22764)

You have two options for installing this security update:

Via the MA-SV GUI, using a Patch file (verodin_sec_update_4.8.2.0.patch). This requires you to be on version 4.8.2.0 or higher.

Via the command line, using a tar.gz file (verodin_repo_4.8.2.0.tar.gz). This method allows you to apply the security patch to any version of the platform.

Instructions for applying the Security Update can be found in Chapter 5.5 of the Admin Guide.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Mandiant

Important Upcoming Changes

The following changes will be made in an upcoming release. Customers are advised to review and prepare for these changes:

- Reminder: Customers with MSV Licenses issued or renewed after January 1, 2022, are ***required*** to execute version 4.8.1.0 or later and maintain a connection to the Mandiant Content Service.
- The https://update.verodinservices.com URL and IP will be retired. Customers will need to ensure their ACLs are updated prior to this change to include the URLs listed below. The exact date of this cutover will be shared in a subsequent update.
    - https://update.validation.mandiant.com
    - https://content.validation.mandiant.com
    - https://telemetry.validation.mandiant.com
- The use of **Integration Event Filters** is discouraged as it will no longer be available or supported in an upcoming release. You should recreate these filters using the new Event Suppression functionality. If that is not possible, please contact your TSC or **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.