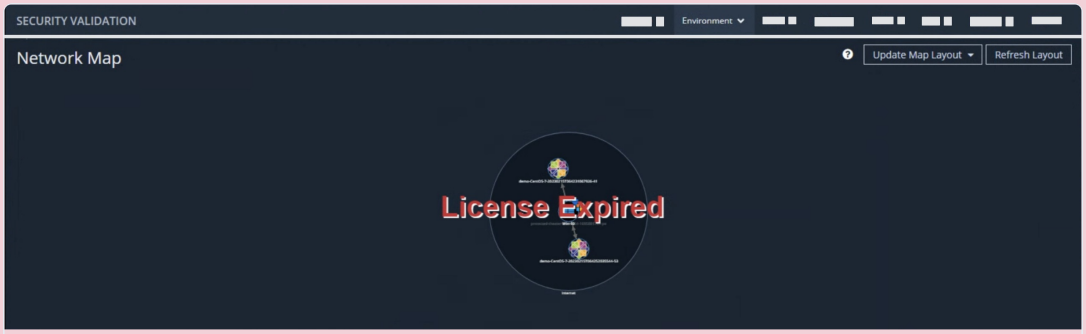
PRODUCT UPDATE 4.10.0.0 - JANUARY 12, 2023

If you're on a Mandiant Security Validation (MSV) release prior to 4.12.1.0, you may notice that a license expired watermark appears on the Network Map page on your Director.



Network Map Page with License Expired Watermark on an MSV Director

This watermark is related to the software that renders the Network Map and does not affect functionality of the product.
Use one of the following options to fix the watermark issue permanently:

- Update to the latest release (4.12.1.0 or later) or migrate to Mandiant Advantage Security Validation (MA-SV).
- As an additional option, you can upgrade to release 4.12.0.1, which provides a fix for this issue and if you need more time to complete the update to 4.12.1.0 or later.

MSV 4.10.2.2 contains defect resolutions and a critical security fix. We recommend you apply that update as soon as reasonably possible. If you're unable to upgrade at this time, use the instructions in **Manage User Admin Account (https://docs.mandiant.com/home/manage-user-admin-account)** to either set a password for the account or disable the account if it's not being used.

This release is Limited Availability, for those requiring the Network Run-As feature.
If you do not need access to this feature, we suggest waiting until this release is made Generally Available.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.10.0.0 of the MSV platform.

General Enhancements

- Added Network Run-As feature

  All Actors need to be updated to 4.10.0.0 to use this feature.

- Added option to include Actor information in Splunk base event queries to improve performance
- Updated Threat Intel API calls to latest versioning

Bug Fixes

- Fixed an issue where suspicious events were not correctly matched to the relevant Job Action
- Fixed an issue where the logs for Protected Theater were not all available for download
- Fixed an issue where Protected Rules were not being managed correctly when there were multiple Protected Theaters

- Fixed an issue where valid network paths were not always showing between Actors
- Fixed an issue that prevented new widgets from being added to reports
- Fixed an issue that sometimes resulted in Protected Theater not being able to update snapshot
- Fixed an issue where summary chart labels were not clearly named
- Fixed an issue that could lead to errors when content generated on one Director was imported to another Director
- Fixed an issue where integration events weren't matching to “updateTime”
- Additional minor bug fixes and improvements

Appliance OS Security Update

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.

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. The criticality of the vulnerabilities resolved are listed below.

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

Details for the vulnerabilities against the Director are as follows:

- CentOS 7: device-mapper-multipath (CESA-2022:7186)
- CentOS 7: krb5 (CESA-2022:8640)

Details for the vulnerabilities against the Actor are as follows:

- CentOS 7: device-mapper-multipath (CESA-2022:7186)
- CentOS 7: krb5 (CESA-2022:8640)

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

- CentOS 7: firefox (CESA-2022:8552)
- CentOS 7: device-mapper-multipath (CESA-2022:7186)
- CentOS 7: xorg-x11-server (CESA-2022:8491)
- CentOS 7: krb5 (CESA-2022:8640)

Important Installation Notes

- Minimum Director version 4.7.0.2 or higher is required to upgrade to version 4.10.0.0.
- Actor Compatibility. Actors must be upgraded to at least version 4.6.0.0 before updating their Director to 4.8.4.1.

To download documentation and software (appliance images, installers, and update packages) visit the **Validation Section of the Docs Portal (https://docs.mandiant.com/home/security-validation-on-prem-and-saas)**. For full details on how to upgrade, see **Updating Security Validation Components (https://docs.mandiant.com/home/msv-system-updates)**.