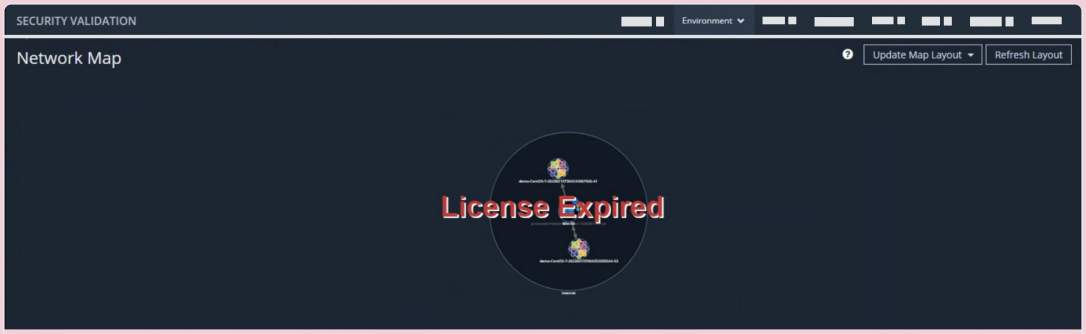
PRODUCT UPDATE 4.11.0.0 - JUNE 20, 2023

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.

The Mandiant Security Validation (MSV) team is pleased to announce version 4.11.0.0 of the MSV platform.

General Enhancements

- Added the Assessments feature (Limited Availability), which simplifies how you get started using content and consistently execute control or compliance assessments across your organization. This feature provides a way to group content together for campaigns, best practices, or quarterly assessments for a compliance audit. See the **Assessments documentation (https://docs.mandiant.com/home/msv-assessments)** for more information.
- Added the Integrations feature (Preview), providing a more modern Integrations solution than in previous releases.
  - This feature is available but disabled by default for appliance-based installations. Contact your TSC or CE if you are interested in enabling and using the Integrations Preview.
  - Given that this feature is disabled by default no additional system CPU or RAM resources will be consumed, but consult the minimum and recommended Director system requirements, outlined in the **Integrations documentation (https://docs.mandiant.com/home/msv-integrations-411)**.
  - If you are using the installer-based deployment and you are interested in using the Integrations Preview, contact your TSC or CE for assistance with a manual upgrade path for the feature. Of note is that the Preview Integrations architecture uses the podman package which must be allowed to install for the feature to install and function.
- Added support for Server Name Indication (SNI) for HTTPS Actions

Bug Fixes

- Fixed an issue where the following API call was not returning any "security_technology": https://app.validation.mandiant.com/v2/jobs/915070.json?only=id,vid,detected,blocked,security_technology
- Fixed an issue that could potentially cause the TAAM integration to Mandiant Threat Intelligence to freeze
- Fixed an issue when running a Network Action where the value of proxy_check was set to true when a proxy was not used. This would have occurred when a source Actor had a default proxy configured but the user overrode the proxy with "None" (value 0).

- Fixed an issue where integration Test query and Operational Status queries would fail due to either a timeout or a buffer overflow caused by too much data
- Fixed an issue where local authentication was still successful after configuring SAML authentication only
- Fixed an issue where the Splunk ES Integration, running on a Remote Integration Actor, would fail when trying to match notable events
- Fixed an issue where Secure Copy Protocol (SCP) file transfer to an appliance Protected Theater would fail
- Fixed an issue where TAAM Evaluations for Host CLI (Windows) included mismatched RunAs tag actions that caused errors during execution
- Fixed an issue where an AEDA Monitor result and Job detail data would conflict

Known Issues

- Unsaved Preview Integration configurations are not prompting users to fill out all required fields first. To work around this issue, double check that values are provided for all the required (*) fields and re-try selecting Save.

Appliance OS Security Update

The latest platform security update can always be found on the **Validation Section of the Docs Portal (https://docs.mandiant.com/home/msv-security-patch-downloads)**. This security update applies to all versions of the product and are cumulative.

Important Installation Notes

Minimum Director version 4.9.0.0 or higher is required to upgrade to version 4.11.0.0.

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)**.