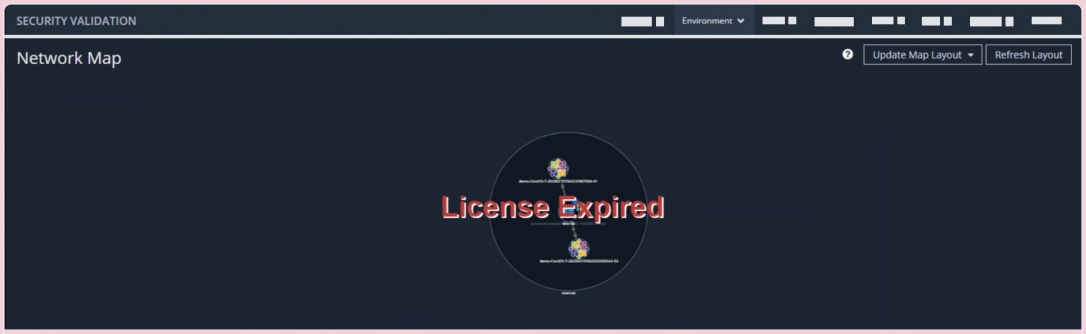
PRODUCT UPDATE 4.10.3.0 - MAY 18, 2023

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 4.10.3.0 of the MSV platform.

General Enhancements

- Improved memory usage by the Job Results API
  - The `GET /jobs/<ID>` API endpoint no longer includes the `integration_events.untranslated` field by default, and truncates the `integration_events.raw_event` field by default to a max of 1024 characters. If users still need those full fields in the response, they can add the included query parameter:

    ```
    GET /jobs/<ID>?include=integration_events.untranslated,integration_events.raw_event
    ```

- When a deleted user tries to authenticate, they now receive a message that their account was deleted and to contact an administrator instead of an authentication error
- Added additional API documentation to pull and filter Director Audit Logs
- Security enhancements

Bug Fixes

- Fixed an issue where the AEDA Dashboard was displaying Monitors as passing when they did not run correctly
- Fixed an issue where the AEDA "Last Run" was not linking to the last run job
- Fixed an issue where the user interface was unable to display the Jobs page with a 414 error
- Updated Security Technologies to include "Trellix"
- Fixed an issue when turning on Active Directory Authentication; users can now see and test new settings prior to rebooting
- Fixed an issue where older exported content would cause the Action Library to crash
- Fixed an issue where security patch updates were failing to apply on some Actors
- Fixed an issue in AEDA where altering any existing monitor setting unintentionally changed the proxy being used by the Monitor

- Fixed an issue where log rotation was not properly working on Remote Integration Actors
- Fixed an issue where users with System Admin roles were not able to delete user-created evaluations
- Made improvements to prevent Bad Request integration errors when queries were above a certain size
- Fixed an issue where users were unable to add sleep Actions when creating an Evaluation from the API

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 4.8.4.0 or higher is required to upgrade to version 4.10.3.0.

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)**.