PRODUCT UPDATE 4.8.4.0 - JULY 12, 2022

The Mandiant Security Validation (MSV) team is pleased to announce availability of version 4.8.4.0 of the platform. This release adds several new and enhanced capabilities to the Validation Platform, including *Integration enhancements, expanded data access, 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 4.8.4.0.
- Actor Compatibility. Actors must be upgraded to at least version 4.6.0.0 before updating Director to 4.8.4.0.

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)**. The previous Security Validation Customer Portal, msv.mandiant.com, is retired and does not contain the 4.8.4.0 updates.

Important Update Regarding Security Updates

As of 4.8.4.0, all new Actor, Director, and Protected Theater appliances deployed will have automatic OS package updates enabled by default, pointing to public CentOS repositories. Customers are asked to **enable automatic package updates (https://docs.mandiant.com/home/msv-security-updates)** on their existing deployed appliances, pointing either to the public repositories or an internal CentOS mirror, or to switch to installer-based deployments on an operating system configured to receive security updates from the OS vendor (e.g. Red Hat/RHEL or Canonical/Ubuntu). New security update packages will continue to be published, on a yet-to-be-determined schedule.

General Improvements and Bug Fixes

Actor/Actions

- Bulk jobs now can be scheduled and repeated
- SELinux enforcing mode support for Actors
- A script used to reset proxy credentials is now installed with the windows actor by default
- Host CLI Actions running on endpoints with the French character set enabled now correctly display blocked status
- Proxy definitions are now applied consistent with override option specified
- Tags now save correctly when Actors are added to the system

Data Access

API

- Added 'start' and 'length' parameters to the Search API
- Added pagination and filters to evaluation page for enhanced page load and search times
- Action errors no longer masks began_at field which had made it difficult for external debugging on "Return Actions related to a Sequence / Evaluation by VID" endpoint
- Improved consistency of responses for ID and VID Lookups from "Lookup Action info by ID or VID" endpoint

CSV Exports

- The job status page now includes errored jobs with exports
- Issues resulting in a malformed CSV export have been resolved
- The Users table can now be exported as CSV

Content

- When authoring custom content, variable substitution will be applied to the success match clause
- Users can now cancel and restart the content import process if needed
- MITRE ATT&CK v10 support in Actions. Tactics for actions now show in a details table in the Action Library. JobResult

exports now contain MITRE ATT&CK techniques and tactics.
- New UX for action creation and editing
- Cleanup commands can now be defined in a separate step using a different user and permission level
- A new status of “Incompatible” has been introduced, which enables content to have a pre-execution check to determine if the action applies to the target environment

Protected Theater

- Enhanced support for Protected Action Desktop Screenshots
- Support Windows Defender Dynamic Ruleset
- Removed default “pool.ntp.org” NTP servers from Actor/Protected Theater Appliances
- Addressed various issues related to Protected Theater rollbacks and logging
- Protected Actor actions or upgrade are no longer allowed during Protected Theater upgrade (and vice-versa)

Events and Reporting

- Actions labeled with T1043, a deprecated MITRE v6 technique, have been updated
- Improved validation for Search fields in report builder
- New report builder widgets for “Force Field” and “Bullet” / “Column” charts
- PDF rendering and whitespace removal have been further optimized
- Ability to separate different types of events from the same security product. For instance, a next-generation firewall with traffic events and URL filtering can be represented as ‘NGFW Traffic’ and ‘NGFW URL Filtering’ for event matching and reporting
- Proxy addresses are now used in both the query and matching for events from integrations

Integrations

- Splunk: Sporadic high latency queries associated have been resolved
- QRadar: A data mismatch issue was resolved
- Darktrace: Improved exception handling when non-UTC time zones are used
- Cisco FMC: An error preventing the integration test from executing successfully was resolved.
- Threat Intelligence Platform (TIP) sync time settings can now be modified

Diagnostics

- Actor pull logs from a Director now include more Actor details to make it easier to associate with a given Actor
- Actor conversation logs now include proxy IP address for any proxy communications to assist with integration event matching

General UX Improvements

- Performance improvements loading the Library for Actions, Sequences, Evaluations, and Files
- Enhanced stability of resized modal page elements
- Map improvements for Actions between Actors when Allow Actions between All Actors selected
- Users can now select which version of MITRE Tags they prefer to work with via the advanced settings page and via API.

General Bug Fixes

- Updated TLS/SSL Service DH Parameters for enhanced security
- Resolved issue with Actors where unexpected system proxy settings could cause Director connection failures
- System backup files now removed after 3 days
- SSL certificate requests in Director Console now create server.csr file
- Strengthened ciphers in HTTP server configuration
- Test Interface now supports binding to Port 80
- Proxy addresses are now used in both the query and matching for events from integrations
- Multiple fixes for NTLM HTTP proxy support

- Support for Customer Actor iptables on Linux Actors
- Jobs settings now persist across multiple job runs
- Restored cleanup of action files on Actor upgrades
- Directors will no longer request log files from Actors that are down
- Support for updating Monitors to run between Zones
- Improved consistency of JSON and Job data exports
- Updated Operational Status Actor NTP check test to only run for CentOS7 actors