PRODUCT UPDATE 5.10.1.0 - FEBRUARY 16, 2023

The Mandiant Advantage Security Validation (MA-SV) team is pleased to announce version 5.10.1.0 of the MA-SV platform.

General Enhancements

- Added option to include Actor information in Splunk base event queries to improve performance
- Updated Threat Intel API calls to latest versioning
- Added ability to match integration events using "updateTime"
- New users now must be configured in Mandiant Advantage SSO rather than the Settings UI in MA-SV
- Email Theater Actions now report SMTP ID of emails sent by Jobs
- Added support for MITRE ATT&CK version 12.1
- Added support for Credential Cache for proxy configurations
- Improved memory utilization for several processes to improve Director performance

Bug Fixes

- Fixed an issue where some evaluations were not run due to missing binaries.
- Fixed an issue where the heat map API documentation referenced incorrect field names
- Fixed an issue where the listed AEDA last run monitor was incorrect
- Fixed an issue that resulted in an incorrect status for Host CLI jobs run against French endpoints
- Fixed an issue where Windows Endpoint Actors were not always updating IP information in Director
- Fixed an issue regarding Host CLI timeout behavior
- Fixed an issue where Daylight Savings introduced a 1-hour time skew for some jobs
- Fixed an issue where an Internal Server Error occurred when running some Evaluations
- Fixed an issue that caused bulk registration tokens to expire
- Improved DNS matching for some Evaluations
- Fixed an issue where Host CLI commands would disappear or be modified with cleanup
- Fixed an issue where AEDA webhook variable expansion was not JSON compliant
- Fixed an issue where Host CLI actions would error when run as an Active Directory user
- Fixed an issue where the Chronicle integration was missing the ability to select between version 1 and 2 for on-prem Directors
- Fixed an issue that caused Protected Theater Evaluations to error out after partial completion
- Fixed an issue where some security technologies would stop communicating with Protected Theater
- Fixed an issue where integration queries were being erroneously replicated and causing memory problems
- Fixed an issue where Actor communications were being interrupted by cleanup processes
- Made various improvements to MSFT Graph API calls
- Fixed an issue where SAML login was not working with Azure AD
- Fixed an issue where the date/time filter on the Jobs page would incorrectly work for "Today"
- Improved Operational Status Graph performance and long load times
- Additional minor bug fixes and improvements