JUNE 29, 2022 MANDIANT ADVANTAGE THREAT INTELLIGENCE RELEASE

New Versions

- Mandiant Advantage Threat Intel (MATI) v2.5.8
- Mandiant Advantage API (MAAPI) v1.28.5
- Mandiant Advantage Digital Threat Monitoring (DTM) v1.45.3

New in this Release

MATI / MAAPI

- Mandiant Threat Intelligence users can now manage Email Delivery Profiles to get Mandiant Intelligence updates delivered to their inbox. They can select specific types of profiles to receive, choose daily or hourly frequency of delivery, set the delivery time, and manage multiple profiles.
    - Email Delivery Profiles are accessible from the "Email Delivery Profiles" section of the "Settings" page.
- File Analysis--
    - Improved support for archive files containing multiple files. The results of the File Analysis now present information for the individual files included in the archive.
    - Addition of the "Ask an Expert" option to allow the user to ask for help directly from the File Analysis section.
- In search results, tools are now labeled "Tools" and use the tools icon (where labeled "Malware" in previous editions).
- Expertise on Demand subscribers: Access to Service Description and List of Services documentation from the EOD subscription card ("Settings" tab)
- Replaced the News & Analysis widget in "Reports & Analysis" dashboard, "Actor Details", "Malware Details", and "Tools Details" pages with a new widget and tooltip.

DTM

- Made minor UI enhancements on--
    - Alert Details page
    - Monitor List page
    - Research Tools
    - Monitor Templates
- Scaled Alert Detail view to full height on browser.
- Added ability to pivot from a Monitor to its Alerts.
- Added ability to see number of Alerts generated for each Monitor based on date range.

Bug Fixes

MATI / MAAPI

- Info Ops & Hacktivism filter now returns Reports.
- Fixed issue of Vulnerabilities being searchable by UUID, but not CVE.
- Fixed issue of Customer Admin users incorrectly defaulting to Free when added.
- News Analysis on the News Ticker no longer displays outdated reports.
- Fixed issue with MITRE ATT&CK Explorer only allowing selection of one Sub-region.
- /v4/ reports endpoint now returns a page token.
- POST /collections/indicators/objects no longer returns a method not allowed response.

DTM

- Improved handling of comma lists in Monitor condition values.
- Email settings are now fetched each time settings are opened.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Fixed issue of blank screen after some searches.
- Fixed invalid link to Lucene query syntax on Monitor creation.
- Monitor list page now refreshes when monitor is created / deleted or enabled / disabled.
- Fixed issue with Research Tools and Alerts since [date] calling API incorrectly.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.