Mandiant

SEPTEMBER 26, 2023 MANDIANT ADVANTAGE THREAT INTELLIGENCE RELEASE

New Version

- Digital Threat Monitoring (DTM) v1.136.4

New in this Release

- **Compromised Credentials Monitoring**
  - New Monitor detects the presence of specific user accounts in compromised credentials data collected from the deep and dark web. This feature replaces Credential Leaks monitoring, which detected mentions of leaked credentials in chat messages, forums, and documents found on the web.

    For more information, see **Monitor Compromised Credentials (https://docs.mandiant.com/home/dtm-monitor-compromised-credentials)**.

- Updated **Domain Discovery** Alert titles to improve clarity and readability by incorporating a comma-separated list of matched keywords.
- Research Tools now supports searching CIDR ranges for `ipv4_address` and `ipv6_address` entities.
- Research Tools now supports searching CIDR ranges for `group_network` entities.
- Research Tools now supports search of nested documents and fields.
- Implemented Path Analyzer for path entities to improve Monitor usage and searchability from Research Tools.

Bug Fixes

- Correct monitor version is now shown in the Raw JSON of an Alert.
- Fixed an issue where some Research Tools documents loaded a blank page with an error.
- Content from **Pastes** Alert types is now showing in the **Rendered View** tab instead of the **Raw Text View** tab.
- Fixed instances of match path checks that were hardcoded to only check the first item in an array.
- Resolved issue that caused blank alerts.