Mandiant

MANDIANT SECURITY INTEGRATIONS (MSI) SERVICE

The availability of the latest MSI release depends on which Security Validation environment you're using:

- Mandiant Advantage Security Validation (MA-SV) customers are automatically updated to the latest MSI version as soon as it's released.
- Mandiant Security Validation (MSV) customers need to update their MSI version by applying the latest available security update that contains a new MSI version to their environment.

Security updates may be released one or two days after the MA-SV update. See the following documents for more information:

- **Security Update Downloads (https://docs.mandiant.com/home/msv-security-update-downloads)**
- **Apply Security Updates to your Security Validation Appliances (https://docs.mandiant.com/home/msv-security-updates)**

Recent releases

MSI 2.0.5.1 - October 6, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- **Carbon Black Cloud v1:** Migrated from deprecated Alerts API `v6` to Alerts API `v7` search endpoint (`/api/alerts/v7/orgs/{org_key}/alerts/_search`) and updated health check endpoints.
- **MSI Requests:** Extended async authentication and proxy handling for Google-based integrations.
- **Trend Micro Vision One v1:** Added support for querying `/v3.0/search/endpointActivities` when enabled through the `searchEndpointActivities` runtime configuration.
- **Trend Micro Vision One v1:** Updated integration branding and UI logo to Trend AI.
- **Pure query support:** Added support for Pure Query mode in test queries across multiple integrations:
  - Anomali Security Analytics v1
  - Azure Log Analytics v1
  - CrowdStrike v2
  - CrowdStrike Falcon LogScale v1
  - CrowdStrike Next-Gen SIEM Search v1
  - Elasticsearch v1
  - Google BigQuery v1
  - Google Chronicle v1
  - Google Cloud Logging v1
  - LogRhythm Elastic v1
  - QRadar v1
  - SentinelOne v1
  - Trellix Helix v1
- **Performance optimizations:** Migrated several integration handlers to asynchronous architectures:
  - Exabeam Analytics v1
  - Google Chronicle v1

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- **Deprecations:** As of this release, the following integrations are deprecated:
  - VMWare AppDefense v1
  - Security Onion Elsa v1

Bug fixes

- **Azure Sentinel v1:** To prevent malformed queries or API exceptions from halting subsequent query executions, wrapped query execution in error handling.
- **Microsoft Graph Security v1:** Fixed an `Invalid audience` (`InvalidAuthenticationToken`) authentication error in Azure Government Cloud environments by dynamically using the configured host for token scope rather than a hardcoded commercial endpoint.
- **MSI Base Java:** To address security vulnerabilities, updated OpenJDK base image to version `25.0.4.1+1`.
- **MSI Requests:** Fixed an issue where `expires_in` string representations caused failures during OAuth `async_auth`.

MSI 2.0.5.0 - September 9, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

New integration

- **FORTINET FortiSIEM**

Enhancements

- **Async conversion updates**: To improve performance, responsiveness, and request handling, migrated several integration handlers to asynchronous architectures. Affected integrations include the following:
  - ArcSight v1
  - Carbon Black Response v1
  - Crowdstrike V2
    Exabeam Cloud v1
  - LogRhythm Cloud v1
  - MS Defender ATP V1
  - Splunk V1
  - Trellix Helix v1

- **Enabled support for SSL certificate authentication** for the following integrations:
  - Carbon Black Response v1
  - Cybereason v1
  - LogRhythm Cloud v1
  - SentinelOne v1
  - Trellix Helix v1

Bug fix

- **Trellix ePolicy Orchestrator v1**: Fixed default query formatting
- Improved software supply chain security by enforcing strict checksum and integrity verification on third-party libraries used within integration environments.

MSI 2.0.4.5 - August 11, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- **Azure Sentinel:** Enabled support for SSL certificate authentication capabilities.
- **Async conversion updates**: To improve performance, responsiveness, and request handling, migrated several

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

integration handlers to asynchronous architectures. Affected integrations include the following:

- Azure Log Analytics v1
- Azure Sentinel v1
- Checkpoint v1
- Cisco Firepower v1Cisco Firepower v2 Elasticsearch v1
- SentinelOne v1
- Trend Micro Trend Vision One v1

Bug fixes

- **Trellix Email Security Cloud:** Resolved miscellaneous authorization and connectivity issues.
- **RSA NetWitness Logs & Packets:** Fixed the expansion of multi-value query variables (such as `%IPS%` and `%HOSTNAMES%`) to ensure they correctly expand as comma-separated lists, preventing query syntax errors.
- **AlienVault:** Resolved an issue that was caused by an invalid structure in the default field mapping.
- **Default query formatting:** Corrected default query formatting for the following integrations:
  - Palo Alto
  - Trellix EDR Threats
- **Framework:** Resolved a typing issue during OAuth2 requests to improve authentication reliability.

MSI 2.0.4.4 - July 15, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- **Trend Micro Vision One v1:** Exposed the query configuration in the runtime settings. With support for placeholder substitution for `%IPS%` and `%HOSTNAMES%`, users can configure custom queries for IP and hostnames.
- **Palo Alto Cortex XSIAM v2:** For better clarity, updated the default queries format to include titles.
- **Tipping Point v1:** Updated the default queries format to include titles for better clarity and identification.
- To improve readability and consistency in the Director interface, added titles to default queries across several integrations. Affected integrations include the following:
  - Graylog v1
  - Rapid7 InsightIDR v1
  - Juniper JSA v1
  - RSA NetWitness Logs & Packets v1
  - Symantec DLP v1
  - Trellix Email Security Cloud v1
- **Framework:** Updated the underlying Java environment to OpenJDK 25.0.3 (msi-base-java).

Bug fixes

- **Trellix ETP:** Resolved a crash (`'HttpAuthProxyConfig' object has no attribute 'get'`) during OAuth token retrieval when a proxy was configured.
- **Splunk v2:** Fixed an issue that prevented the expansion of the `IN (%IPS%)` variable in event queries, ensuring multiple IP addresses are correctly formatted as `IN ("IP1", "IP2", ...)`.
- **Azure Sentinel:** Resolved an HTTP 400 Bad Request / SemanticError (`Left and right side of the logical expression must be Boolean`) that occurred during DNS event queries containing the `%DOMAINS%` variable.
- **Elasticsearch:** Fixed a validation error that occurred when using or copying the default Alert Query in the test query interface.

MSI 2.0.4.3 - June 17, 2026

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Bug fixes

- Fixed an issue with an RPM error.

MSI 2.0.3.0 - June 9, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- **Trend Micro Vision One v1:** Exposed the Alert Field Mapping configuration in the web interface, allowing users to customize which fields are used for alert data. Default mappings are still provided.
- Enabled support for SSL certificate authentication for the following integrations:
  - **Exabeam Cloud v1**
  - **Splunk v1**
  - **Splunk v2**
- Added titles to the default queries for the following integrations:
  - **Google BigQuery v1**
  - **Logzilla v1**
  - **Microsoft Defender ATP v1**
  - **Security Onion v1**
  - **Trellix Enterprise Security Manager v2**
  - **Trellix Enterprise Security Manager v1**
  - **Trellix Helix v1**

Bug fixes

- **Cybereason v1:** Fixed an issue where Default Malware Queries were not displaying, which prevented the integration from being saved. This was due to incorrect model typing for the malware queries field.
- **Google Cloud Logging v1:** Fixed an `AttributeError` that occurred during health checks when a Service Account JSON was provided as a string instead of a parsed object. The integration now correctly handles the JSON input.
- **LogRhythm Elastic v1:** Removed invalid `0` values from the default field mapping, which caused errors when saving the integration.
- **Microsoft Graph API v1:** Corrected the expansion of `%HOSTNAMES%` and `%IPS%` variables when multiple values are present. Each value in the list is individually single-quoted, ensuring correct query syntax,
- **Trellix Helix v1:** Resolved an integration failure caused by incorrect authentication scopes.
- **Framework:** Resolved an issue preventing integrations with proxies from being saved or edited.

MSI 2.0.2.0 - May 11, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- SentinelOne v1: Added support for the Alerts API (`/web/api/v2.1/cloud-detection/alerts`). This allows the integration to fetch alerts triggered by custom or default STAR Rules, in addition to the existing support for Threats.
- Google Chronicle v1: Enabled support for SSL certificate authentication, providing an additional method for secure connections.
- Framework: Updated the field mapping description to include information about the new Complex Field Mapping

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

capability, which allows for string concatenation using the + operator.

Bug fixes

- Securonix v1: Fixed an issue where default queries were not appearing when configuring a new Securonix integration.
- AWS CloudWatch v1: Resolved an exception that occurred when the logGroupName parameter was missing or null. The handler includes early validation to check for this parameter.

MSI 2.0.1.1 - April 28, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Google Chronicle v1**:** Updated the web interface readme and customer documentation to include instructions on permissions that are required for using the optional Service Account Impersonation.

Bug fixes

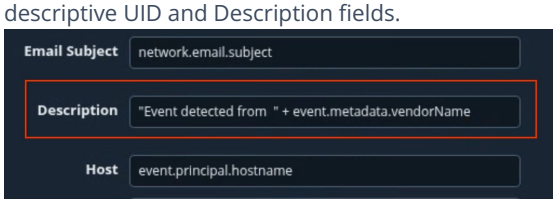
- Darktrace v1: Corrected a type mismatch in the queries field to ensure that queries can be saved and run correctly.

MSI 2.0.1.0 - April 20, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- General:
-
    - Added support for complex field mapping. This feature lets you construct a single field's value by combining static strings and values from multiple other fields within the event data. This is useful for creating more descriptive UID and Description fields.



    - Added version logging to the `/health` endpoint. The current MSI version is logged when the health check endpoint is called.

- Google Chronicle v1**:** Updated the default field map for the `url` field to ensure it uses a valid field.
- Palo Alto v1**:** For compatibility reasons, removed the Strata Cloud option. If you used this, you need to switch to the firewall or panorama console device type.
- MS Graph Security v1: Added complete variable configuration support.

Bug fixes

- Splunk v2: Resolved an `AttributeError` in the query handler. The issue was caused by the code incorrectly expecting a list of messages from the Splunk API, while a dictionary is actually returned.

MSI 2.0.0.0 - March 31, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Elasticsearch v1: Added support for API key authentication.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Microsoft Defender ATP v2: Added support for SSL certificate validation.
- Palo Alto Cortex XSIAM v2 (Preview): Added support for the new XSIAM 3.0 APIs.

Bug fixes

- Splunk v1 & v2: Resolved an issue to better handle "Premature Peer Termination" errors that Splunk receives.

MSI 1.8.0.6 - March 17, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Crowdstrike v2: Modified required scopes in embedded documentation to reflect `Alerts: Read`.

Bug fixes

- Exabeam: Fixed an issue where correlation rules were not matching to job actions.

MSI 1.8.0.5 - March 2, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Crowdstrike v2
  - Updated the Field Map information text to accurately reflect the fields used for the `__default__` value.
  - Enhanced the default Field Map for `start_time` by adding `timestamp` as the primary option and `original_start_time` as the secondary option.
- Splunk
  - Improved error handling for cases where the Splunk server is overloaded.
  - Added a time modifier to the default IP query to optimize search performance and consistency with other default queries.

MSI 1.8.0.4 - February 11, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Microsoft Graph Security: Updated the API permission text in the web interface to specify `SecurityAlert.Read.All` instead of `SecurityEvent.Read.All`.
- Crowdstrike v2: Removed references to the decommissioned Incidents API. For changes to the default field map values, see the following table:

MSI Default Field Map Name	Previous Default	Updated Default
uid	`behavior_id`	`composite_id`, `id`
src ip	`ip_address`	`device.local_ip`, `device.external_ip`
src port		`device.local_port`
dest port		`device.remote_port`
start time	`timestamp`	`created_timestamp`, `context_timestamp`

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

MSI Default Field Map Name	Previous Default	Updated Default
sid	behavior_id	user_id
url		falcon_host_link
description	__default__	__default__ , description , automated_triage.triage_explanation , triage_explanation , priority_explanation
host	host	device.hostname , host_names.0
computer	domain	domain , device.hostinfo.domain , device.machine_domain
user	user_name	user_name , user_principal , parent_details.user_name , grandparent_details.user_name , logon_domain
filehashes		sha256 , md5 , ioc_context.sha256 , parent_details.sha256 , grandparent_details.sha256

MSI 1.8.0.3 - January 26, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Azure Log Analytics: Added more logging, including logging for variable replacements.

Bug fixes

- Azure Sentinel: Resolved an issue with NTLM proxy authentication by enforcing session persistence.
- Azure Log Analytics: Resolved an issue with NTLM proxy authentication by enforcing session persistence.

MSI 1.8.0.2 - January 6, 2026

This release note outlines the latest updates, enhancements, and bug fixes for the Mandiant Security Integrations (MSI) service.

Enhancements

- Microsoft Graph Security: Updated the alert endpoint to use the new alerts_v2 API.
    - The default field map values have been updated, therefore:
        - Any new Microsoft Graph Security integration uses these new defaults.
        - Existing integrations will need to be edited to use the new field map values.
- Trellix Helix and Trellix Email Security Cloud: Added the ability to select between Trellix IAM (Oauth2) and FireEye IAM (API key).
- Alert Logic: Added health check.
- CloudWatch: Improved error handling and logging.
- Microsoft Defender ATP v1 and v2: Added a warning message when the API limit is returned from the API. Events that have been retrieved before reaching the limit are still returned.

Bug fixes

- Google Chronicle v1: Fixed an issue preventing updates to the integration from the web interface.
- Microsoft Graph Security: Improved error handling for runtime errors.
- Crowdstrike: Fixed SSL issue for SSL certificate upload and usage.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Netskope v2: Fixed attribute error by utilizing the correct `host` from `conn_config`.

Archived releases

MSI 1.8.0.1 - December 8, 2025

Enhancements

- Anomali Security Analytics: Added error handling for runtime errors if a job query does not complete.
- Palo Alto XDR: Updated to apply a unique identifier to alert events if a uid is not found.
- Palo Alto XSIAM: Updated to apply a unique identifier to alert events if a uid is not found.
- VMWare: Updated to use dynamic field mapping.

Bug fixes

- Crowdstrike: Fixed SSL certificate usage.
- VMWare: Fixed a typo in the readme/about.

MSI 1.8.0.0 - November 17, 2025

Enhancements

- Upgraded embedded Python components to version 3.12

MSI 1.7.8.1 - November 10, 2025

Bug fixes

- Crowdstrike: Fixed an issue where MSI wasn't able to verify an SSL certificate because of a proxy requiring a custom CA certificate.
- SentinelOne: Fixed an issue where the default query returned an error when `%HOSTNAMES%` was in the query.
- XDR: Fixed an issue where events weren't correlated properly, resulting in incorrect metrics.

MSI 1.7.8.0 - October 21, 2025

New integrations

- **Splunk 10.x (API V2)** **(https://docs.mandiant.com/home/msv-splunk-integration)**
- **Google Chronicle V1** **(https://docs.mandiant.com/home/msv-google-chronicle-integration)**

Enhancements

- AWS CloudWatch: Added an SSL certificate upload field.
- Crowdstrike: Updated the API requirements information in the V2 readme.
- Google Chronicle Backstory: V2 API is deprecated.
- Splunk 10.x (API V2): Integration includes risk notables.

Bug fixes

- Fixed an issue where an MSI Integration showed the last run query with invalid characters and translated them incorrectly.

MSI 1.7.7.0 - October 6, 2025

Crowdstrike v1 has been deprecated and is no longer supported.

Enhancements

- Darktrace v1: Added the ability to run advanced queries.
- SQL v1: Added health check.

Bug fixes

- Google Chronicle Backstory v2: resolved the NoneType Error seen in logs if no queries were defined.
- Checkpoint v1: Removed unnecessary time options.

MSI 1.7.6.0 - September 24, 2025

Enhancements

- Palo Alto Next-Gen Firewall: Added support for the Strata Cloud Manager appliance.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Bug fixes

- Fixed an issue where Trellix products were missing from the Security Technology Definition menu.
- RSA Netwitness: Fixed the time format for `%START_TIME%` and `%END_TIME%` values in logs and packets.
- Exabeam: Fixed an issue where alerts weren't being populated from MSV.

MSI 1.7.5.7 - September 8, 2025

Enhancements

- Chronicle Backstory: Missing queries are logged instead of being raised as an exception.
- Palo Alto: In queries, added an AND type join for IP addresses.

Bug fixes

- Qradar: Fixed an issue where the integration wasn't pulling alert events but was getting base events.

MSI 1.7.5.6 - August 25, 2025

Bug fixes

- AWS CloudWatch: Fixed an issue where queries were failing if they were not in JSON format.
- ExtraHop Reveal 360: Fixed an issue with the default query.
- Google Chronicle Backstory: Fixed an issue where variables in the additional fields did not expand.
- LogScale: Fixed an issue where queries were failing because of a timestamp conversion calculation.

MSI 1.7.5.5 - August 4, 2025

Bug fixes

- Trellix Helix: Updated to use the appropriate value joiner for variables.
- LogRhythm Elastic: Updated to use the appropriate IP joiner for the %IPS% variable.

Enhancements

- Palo Alto: Added support to use any field to expand IPs in queries. For example, addr.src in %IPS%.
- Exabeam Cloud: Updated Alert handling and made correlation query configurable.

MSI 1.7.5.4 - July 24, 2025

Bug fixes

- Chronicle Backstory (Google SecOps): Fixed an issue where an exception appeared when a variable had no values to expand.

MSI 1.7.5.3 - July 7, 2025

Enhancements

- Chronicle Backstory (Google SecOps): Added changes to let users write their own search queries. Default queries are provided that can be customized.
- Google BigQuery: Added setting to allow usage of LegacySQL.

MSI 1.7.5.2 - June 30, 2025

Enhancements

- BigQuery: Made improvements to error message handling.
- Palo Alto Networks Cortex XSIAM: Added this entry to Security Technologies.
- Splunk: The last run correlation query appears in the Director web interface.

Bug fixes

- LogRhythm: Fixed an issue related to elastic queries.
- CrowdStrike Next Gen SIEM: Fixed an issue where failed queries resulted in empty lists instead of error messages.

MSI 1.7.5.1 - June 9, 2025

Enhancements

- MS GraphQL: Added support for the `runHuntingQuery` API endpoint.

Bug fixes

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- LogRhythm Elastic SIEM: Fixed an issue where a query string wasn't getting properly parsed into JSON.

MSI 1.7.4.0 - May 28, 2025

Enhancements

- Snowflake: Added key-pair authentication
- Google Chronicle Backstory: Added a User Defined Query field.
- Added correlation queries under the MSI integration test view.

Bug fixes

- Trellix Helix: Fixed an issue where the wrong header was being used.
- Cisco Advanced Malware Protection: Fixed an issue where the integration URL was incorrect.

MSI 1.7.3.2 - May 12, 2025

Enhancements

- The following integrations, which use OAuth2 authorization, have been updated to add proxy support:
  - Crowdstrike
  - Crowdstrike Next-Gen SIEM Search
  - Crowdstrike Threat Intel
  - Extrahop Reveal 360
  - Google Chronicle Backstory
  - Microsoft Graph API

MSI 1.7.3.1 - April 24, 2025

Enhancements

- Palo Alto Next-Gen Firewall: Updated the logging level.

MSI 1.7.3.0 - April 21, 2025

New integrations

- **Crowdstrike Next-Gen SIEM Search** **(https://docs.mandiant.com/home/msv-crowdstrike-ng-siem-search-integration)**

Enhancements

- Trellix EDR Threats: Added a **Scope** field so user can add any desired scopes for the request.

Bug fixes

- Trellix ESM: Fixed an issue with error handling and an early session logout.

MSI 1.7.2.5 - April 7, 2025

Enhancements

- CrowdStrike: Update the v1 and v2 documentation to include the required permissions for the API key.

Bug fixes

- Fixed an issue for multiple integrations where the Health Check showed a Healthy status even though the integration wasn't configured correctly.

MSI 1.7.2.4 - March 25, 2025

Bug fixes

- AWS integrations: fixed proxy-related issues.
- Microsoft Defender for Endpoint: Fixed an issue where a JSON decode error appeared when getting events.

MSI 1.7.2.2 - March 10, 2025

Enhancements

- Trellix EDR: Moved this technology listing from Network to Endpoint integrations.

Bug fixes

- Fixed an issue where the default fields for Elasticsearch were incorrectly set.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

MSI 1.7.2.1 - February 26, 2025
Bug fixes
- Anomali Security Analytics: Fixed an issue related to query results and added optional configuration for sleep time between API calls for query results.

MSI 1.7.2.0 - February 20, 2025
New integrations
- **Anomali Security Analytics (public preview)** **(https://docs.mandiant.com/home/msv-anomali-sa-integration)**

Bug fixes
- Arcight: fixed an issue where the password was revealed in the `verodin_msi_log` file.

MSI 1.7.1.1 - February 12, 2025
Bug fixes
- Netskope V2: Fixed an issue where the proper key was not used in API response to return events.
- Security Onion ELK: Fixed an issue where `page_size` and `max_pages` parameters weren't passed for Queries.

MSI 1.7.1.0 - February 6, 2025
New integrations
- **Trellix Endpoint and Detection Response (EDR)** **(https://docs.mandiant.com/home/msv-trellix-edr-integration)**
- **Netskope API v2 (public preview)** **(https://docs.mandiant.com/home/msv-netskope-integration)**

MSI 1.7.0.1 - January 27, 2025
Enhancements
- Secureworks Taegis XDR readme: Improved formatting of the API key prerequisite steps.
- Added an enhancement that removes previous MSI images after an MSI software upgrade is completed.

MSI 1.7.0.0 - January 13, 2025
New integrations
- **Secureworks Taegis XDR** **(https://docs.mandiant.com/home/msv-secureworks-taegis-xdr-integration)**
- **Trellix IPS Manager** **(https://docs.mandiant.com/home/msv-trellix-ips-integration)**

Enhancements
- Google Cloud Logging and Google Big Query: Updated to use service account impersonation.

Bug fixes
- Fixed an issue with running a Health Check on a Sumologic integration.

MSI 1.6.6.7 - December 16, 2024
Enhancements
- Cisco FMC: Added support for queries on versions 7.2.7 and later.

Bug fixes
- AWS integrations: Fixed an issue where the Health Check failed when a proxy was involved.

MSI 1.6.6.5 - December 4, 2024
Bug fixes
- Azure Sentinel: Fixed an issue where the integration wasn't pulling events.

MSI 1.6.6.4 - November 19, 2024
Enhancements
- Exabeam Cloud: Added hostname joiner.
- SentinelOne: Added Field Map options.
- SQL: Removed bind values to parse query with variable placeholders.

Bug fixes
- Trellix Endpoint Security: Fixed an issue related to the filter query.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Azure Sentinel: Fixed an issue related to alerts.

MSI 1.6.6.3 - November 5, 2024
Bug fixes
- SumoLogic: Fixed an issue where session cookies weren't used

MSI 1.6.6.2 - November 4, 2024
Enhancements
- Crowdstrike v2: Updated to support queries
- Palo Alto Cortex XSIAM: Optimized to avoid broad search on test

Bug fixes
- SQL: Fixed an issue where this integration couldn't be saved

MSI 1.6.6.0 - October 16, 2024
New integration
- Crowdstrike v2

Enhancements
- Carbon Black: Updated to v7. Note that v1 and v2 are deprecated and no longer supported.
- Google Cloud Logging: Updated default query and field map.
- Exabeam Cloud: Added alerts.
- AWS integrations: Removed unused port and protocol fields.
- Sumologic: Added cookie authentication.
- Splunk: Improved documentation for Splunk ES Suite support.

Bug fixes
- Exabeam Analytics: Fixed an issue related to session fields.

MSI 1.6.5.1 - October 7, 2024
Enhancements
- Exabeam: Updated get-events to capture alerts.
- AWS Cloud: Added opt-in regions for Cloudtrail, CloudWatch, and GuardDuty.

MSI 1.6.5.0 - September 23, 2024
Enhancements
- CrowdStrike: Added `src_ip` and `dest_ip` values for matched events.

Bug fixes
- Fixed an issue related to HTTP proxy authentication for MSI requests.

MSI 1.6.4.2 - September 16, 2024
Enhancements
- Azure LogAnalytics: Added support for custom OAuth API host
- Palo Alto Next Gen Firewall: Added support for Panorama 11.2

MSI 1.6.4.1 - September 3, 2024
Enhancements
- Cisco Firepower V2 readme: Added more information about v1 and v2 conflicts.

Bug fixes
- Fixed an API authentication issue on Exabeam Analytics.

MSI 1.6.4.0 - August 19, 2024
New integrations
- RSA Netwitness XDR v12

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Enhancements

- Updated Cisco FMC readme with a Support section for switching from v2 to v1 and a note about SaaS support restriction.

Bug fixes

- Fixed an issue where the OpenSearch MSI integration returned an error 427 during a Health Check.
- Fixed an issue where an MSI Trellix Endpoint Security integration wasn't working.

MSI 1.6.3.4 - August 5, 2024

Bug fixes

- Resolved Palo Alto errors with default event count.
- Fixed Splunk errors on notable query.

MSI 1.6.3.3 - July 23, 2024

Enhancements

- Exabeam Analytics: Added API token authentication.

MSI 1.6.3.2 - July 2, 2024

New integrations

- LogRhythm Cloud

Enhancements

- Cybereason: Updated the web interface to indicate support for 16.x - 20.x.
- Azure Sentinel: Improved parsing of Alert Queries.

Bug fixes

- Cisco Firepower v2:
  - Fixed issues related to the default values in field mapping.
  - Added default queries to support v7.2.4+ regarding the CONCAT function (combines table columns into a new field or variable).

MSI 1.6.2.0 - June 17, 2024

Enhancements

- Added email and DNS queries for Sumo Logic integrations
- Added API key authentication to access Exabeam Analytics

Bug fixes

- Fixed an issue with the default query date format for Extrahop Enterprise integrations

MSI 1.6.1.6 - June 3, 2024

Enhancements

- Splunk: changed get-events requests to on-demand to reduce timeout issues.
- Azure Sentinel: Updated field to allow for a custom FQDN.
- Devo: Updated and improved readme content in web interface.
- Palo Alto NGFW: Updated and improved readme content in web interface.

Bug fixes

- Azure Sentinel: alert_queries fix
- SentinelOne: Machine Name parsing fix

MSI 1.6.1.5 - May 13, 2024

Enhancements

- Enhancements to logging and resource utilization

Bug fixes

- Fixed an issue where an ArcSight integration was not returning events

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Fixed an issue where incorrect permissions were documented for Microsoft Defender for Endpoint
- Fixed an issue where a Google Chronicle integration was not working due to incorrect permissions being documented

MSI 1.6.1.4 - March 28, 2024
Bug fixes
- Fixed an issue where a QRadar integration was not returning events

MSI 1.6.1.3 - March 14, 2024
Bug fixes
- Fixed an issue where trying to save a Cybereason integration resulted in an error

MSI 1.6.1.2 - February 22, 2024
Enhancements
- Qradar
- Google Security Command Center
- Palo Alto v1
- Logrhythm SQL: fixed incorrect reference to static method

Bug fixes
- Microsoft Defender ATP

MSI 1.6.1.1 - February 6, 2024
Enhancements
- Logrhythm SQL: Added function to check if an IP value is a string type and cast to bytes before further processing
- Exabeam Cloud: IP translation enhancements

Bug fixes
- Qradar: Fixed an issue where events weren't being returned

MSI 1.6.1.0 - January 23, 2024
- General framework updates

MSI 1.6.0.0 - January 11, 2024
New Integrations
- Snowflake Data Lake

MSI 1.5.0.1 - December 20, 2023
Enhancements
- Elasticsearch: fixed alert query variables

MSI 1.5.0.0 - December 19, 2023
New integrations
- Better Stack Logs

Enhancements
- Microsoft Defender ATP: Updated image path to point to the correct repository

MSI 1.4.2.0 - December 7, 2023
Enhancements
- Netskope: uses http error when upstream call fails
- Splunk: returns 427 when all Splunk jobs fail
- Completely remove all usage of integration app status

Bug fixes

Exabeam Cloud: Added queries to output

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

MSI 1.4.1.0 - December 6, 2023
New integrations
- ExtraHop Networks

MSI 1.4.0.0 - November 28, 2023
Enhancements
- Palo Alto Cortex XDR: added XQL queries
- Palo Alto Cortex XSIAM: added XQL queries
- Carbon Black: updated CB response and protection to beta false
- Trellix EPO: updated UID to be hash of event values, sid to be hash
- Azure Sentinel: updated readme file

MSI 1.3.4.1 - November 8, 2023
Enhancements
- Splunk
  - Fixed spelling error in tool tip
  - Splunk by field parsing
  - Splunk actor info in drilldowns
- LogrhythmSQL
  - Logrhythm SQL integration reads events
- Cybereason
  - Query Model Clean-up

MSI 1.3.4.0 - October 26, 2023
New integrations
- AWS DynamoDB

Enhancements
- Sec Palm: Added /summarize Verb/Action
- Google Chronicle Backstory: Added support for dynamic expiration time for entities
- Google Chronicle Integration: Included suspicious domain in UDM
- Clickhouse: Error message enhancements
- Splunk
  - Added Splunk Search and Replacements checkbox
  - Fixed typo in "Subsearch in Tstats Rules" tool tip text
  - Query enhancements

MSI 1.3.3.0 - October 19, 2023
Enhancements
- Splunk
  - Added Enable Checkbox for Correlation Query
  - Added support for IN(%IPS%)
- Google Chronicle SOAR: Renamed Siempilfy Integration
- Google Chronicle: Added Create/Delete/List YARA Rules
- Sec Palm: /get-remediation Update
- Extrahop 360: Updated Default Query Model Definition

MSI 1.3.2.0 - October 10, 2023
New integrations
- Palo Alto Cortex XSIAM

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- ExtraHop 360

Enhancements

- Google Security Command Center

MSI 1.3.1.1 - October 5, 2023

New integrations

- OpenSearch
- Google Cloud Logging
- AWS Cloud Watch
- ClickHouse

Enhancements

- Tanium
- Palo Alto Cortex XDR
- Trellix Network DLP
- Cisco Firepower
- Trellix Network

Bug fixes

- SentinelOne

MSI 1.2.5.0 - September 11, 2023

New Integrations

- Crowdstrike Logscale (formerly Humio)
- Trend Micro Vision One (Apex)

Enhancements and bug fixes

- Symantec ES bug fixes
- Security Onion ELSA enhancements
- Securonox enhancements
- Sumologic enhancements
- Crowdstrike Threat Intel enhancements
- Trellix Network Security v2 enhancements
- Trellix Network Security v1 enhancements
- VMware AppDefense enhancements

MSI 1.2.4.1 - August 31, 2023

Enhancements and bug fixes

- Microsoft Azure log analytics enhancements
- Symantec ES enhancements
- Palo Alto Cortex XDR bug fixes
- RSA Netwitness logs and packets enhancements

MSI 1.2.4.0 - August 21, 2023

Enhancements and bug fixes

- ElasticSearch Alerts
- Crowdstrike Regional Hosts

MSI 1.2.3.0 - August 14, 2023

New integrations

- Tipping Point

Enhancements and bug fixes

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

- Tanium API v4 Support
- FortiAnalyzer
- Google Security Command Center
- Juniper JSA

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.