**Siemplify Marketplace 15.05 Release Notes**

Published on 12 May, 2021

**RELEASE TECHNICAL DETAILS:**

* This marketplace version can only be installed on **Siemplify 5.1** and up

**Integrations:**

* **ActiveDirectory**
* **ActiveDirectory**
* Added support for multiple groups in actions "Add User To Group" and "Remove User From Group" (TIPG-8320)
* **McAfeeEPO**
* **McAfeeEPO**
* Added new actions "Execute Query By ID", "Execute Custom Query", "Get Endpoint Events", "List Queries", "Execute Entity Query" and "List Tasks" (TIPG-7896)
* **MicrosoftAzureSentinel**
* **Microsoft Azure Sentinel**
* REGRESSIVE! Regression Note - The changes in this version might cause regressive changes, due to the changes in the following actions: List Incidents, List Alert Rules, Update Incident Details, Update Incident Labels. In short: Status values "Draft" and "InProgress" are no longer accepted by the api. Instead of "InProgress", "Active" status can be used. Severity value "Critical" is no longer accepted by the api. Json results were changed because updated endpoints return different data. (TIPG-8098)
* Updated the integration's code to work with Python version 3 (TIPG-8108)
* **Office365ManagementAPI**
* **Office365ManagementAPI**
* Added OAUTH2 Login endpoint url parameter to the Integration configuration. (TIPG-8057)

**Actions:**

* **ActiveDirectory**
* **Set User Password**
* Security enhancement in the "Set User Password" action. (TIPG-7662)
* **MicrosoftAzureSentinel**
* **List Alert Rules**
* List Alert Rules: Due to Azure Sentinel backend changes, Severity value "Critical" is no longer accepted by the api. New action input parameter "Max Rules to Return" is added to limit the number of rules to return. (TIPG-8076)
* **List Incidents**
* List Incidents: Action endpoint is updated due to deprecation. This change might cause regressions in existing playbooks. (TIPG-8072)
* **Update Incident Details**
* Update Incident Details: Action endpoint is updated due to deprecation.This change might cause regressions in existing playbooks. (TIPG-8073)
* **Update Incident Labels**
* Update Incident Labels: Action endpoint is updated due to deprecation, and logic has changed, to add labels on top of the existing ones, instead of replacing them. This change might cause regressions in existing playbooks. (TIPG-8074)
* **Get Alert Rule Details**
* Get Alert Rule Details: Action's JSON result is updated to ensure compatibility with the Siemplify Expression Builder. (TIPG-8077)
* **Office365ManagementAPI**
* **Start Subscription**
* "Start Subscription" action updated to allow to subscribe for Audit.General events (TIPG-8055)
* **Stop Subscription**
* "Stop Subscription" action updated to allow to subscribe for Audit.General events (TIPG-8056)

**Connectors:**

* **MicrosoftAzureSentinel**
* **Incidents Connector**
* Incidents Connector: Connector's logic is updated to gracefully skip incorrectly formatted Azure Sentinel incidents. To better handle these incidents, we recommended migrating to Microsoft Azure Sentinel Incidents Connector V2. (TIPG-8088)
* **Incidents Connector V2**
* Incidents Connector V2: Improved functionality and logic of the connector. (TIPG-8089)
* Incidents Connector V2: Connector's default values for "Max Incidents per Cycle" and "PythonProcessTimeout" were changed. It's also recommended to increase the run intervals between connector cycles to at least 30 seconds instead of default 10. (TIPG-8089)
* Incidents Connector V2: "Max Incidents per Cycle" input parameter was changed to "Max New Incidents Per Cycle", and now controls how many new incidents will the connector request from Azure Sentinel in one connector cycle. (TIPG-8089)
* Incidents Connector V2: New parameter "Max Backlog Incidents Per Cycle" was added to control how many backlogged incidents connector will request from Azure Sentinel in one connector cycle. (TIPG-8089)
* **Office365ManagementAPI**
* **Office 365 Management API Audit General Events Connector**
* NEW! New O365 Management API Audit.General events connector added. (TIPG-8054)
* **Office 365 Management API DLP Events Connector**
* Added OAUTH2 Login endpoint url parameter to the DLP Schema Connector configuration. (TIPG-8309)
* Improved "Office 365 Management API DLP Events Connector" functionality in cases of no data in the specified time interval. (TIPG-8431)
* **QRadar**
* **QRadar Correlation Events Connector V2**
* Improved environment mapping functionality of the "QRadar Correlation Events Connector V2", domain\_name and domain\_id can be used to properly map QRadar domains and Siemplify Environments. Note: this may change existing mapping behavior in both the Environment Field Name and map.json file. (TIPG-8479)
* **Splunk**
* **Notable Events Connector**
* Notable Events Connector: Improved connector's parsing in case of special characters. (TIPG-8432)
* Notable Events Connector: Improved the way base events are fetched. (TIPG-8364)