**Siemplify Marketplace 12.9 Release Notes**

Published on 14 July, 2020

**RELEASE TECHNICAL DETAILS:**

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

**Integrations:**

* **ElasticSearch**
* **ElasticSearch**
* Added libraries to the integration. (TIPG-3916)
* **ElasticSearchV7**
* **ElasticSearchV7**
* Added libraries to the integration. (TIPG-3916)
* **IronPort**
* **IronPort**
* Integration configuration page updated: - added separate fields to specify AsyncOS REST API and SSH ports - added a "Use SSL" checkbox to specify whether AsynOS REST API should be accessed over HTTP or HTTPS. (TIPG-3421)
* **McAfeeESM**
* **McAfee ESM**
* Added support for McAfee ESM version 11.2 and 11.3. (TIPG-3553)
* **MicrosoftTeams**
* **MicrosoftTeams**
* NEW! Added support for different redirect URLs for configuration. (TIPG-3629)
* **RecordedFuture**
* **RecordedFuture**
* Added ability to get information about related entities from enrichment actions. (TIPG-3581)
* Updated output message for enrichment actions, when no entities were found. (TIPG-3549)
* **ServiceNow**
* **ServiceNow**
* Added ability to change the default table that will be used in incidents actions. (TIPG-3439)
* Minor improvements across the whole integration. (TIPG-3584)

**Actions:**

* **AzureActiveDirectory**
* **List Groups**
* Removed the "Order By Field" parameter due to API limitations. (TIPG-2451)
* Added support for pagination and added a non mandatory "Results Limit" parameter to limit the number of groups that are returned by the action. (TIPG-2451)
* **List Users**
* Updated the possible values of the "Order By Field" parameter due to API limitations. (TIPG-2451)
* Added "Mobile Phone" column to the user data table. (TIPG-2452)
* Added support for pagination and added a non mandatory "Results Limit" parameter to limit the number of users that are returned by the action. (TIPG-2451)
* Updated the JSON results example to match the actual returned data. (TIPG-2451)
* **CSV**
* **CSV Search By String**
* Fixed a bug that caused incorrect row count to be returned by the action. (TIPG-3707)
* **IronPort**
* **GetAllRecipientsBySubject**
* Action refactored. Action now supports unicode in email subjects. Action input parameters were updated: - New mandatory action input parameter was added - Search Emails for Last X Days. Parameter has a default value. - New mandatory action input parameter was added - Max Recipients to Return. Parameter has a default value. (TIPG-3191)
* **GetAllRecipientsBySender**
* Action refactored. Action input parameters were updated: - New mandatory action input parameter was added - Search Emails for Last X Days. Parameter has a default value. - New mandatory action input parameter was added - Max Recipients to Return. Parameter has a default value. (TIPG-3422)
* **Ping**
* Action refactored. (TIPG-3423)
* **AddSendertoBlocklsit**
* Action refactored. (TIPG-3424)
* **GetReport**
* Action refactored. In action, mail\_sender\_ip\_hostname\_detail and mail\_incoming\_ip\_hostname\_detail reports work based on Siemplify IP or Host entities; mail\_users\_detail works on Siemplify User entity (with email address). Other reports are working without Siemplify entities. Action input parameters were updated: - New mandatory action input parameter was added - Search Reports Data for Last X Days. Parameter has a default value. - New mandatory action input parameter was added - Max Records to Return. Parameter has a default value. (TIPG-3430)
* **MISP**
* **Get Related Events**
* Added "Events Limit" parameter to limit the number of events fetched by the action. (TIPG-3728)
* **Add Tag To An Attribute**
* Added ability to directly specify in which object of the event to add tag to attribute. (TIPG-2698)
* **Remove Tag From An Attribute**
* Added ability to directly specify in which object of the event to remove attribute. (TIPG-2701)
* **Delete An Attribute**
* Added ability to directly specify in which object of the event to add tag to attribute. (TIPG-2704)
* **McAfeeEPO**
* **Get System Information**
* Added support for tasks that contain Unicode data in their name. (TIPG-1839)
* **MicrosoftTeams**
* **Generate Token**
* Updated error message when URL without code parameter is used for authorization. (TIPG-3630)
* **Wait For Reply**
* NEW! Added new action Wait For Reply. (TIPG-3620)
* **List Teams**
* Fixed List Teams to work with unicode (TIPG-3914)
* **List Users**
* Fixed List Users to work with unicode (TIPG-3915)
* **SentinelOneV2**
* **Create Path Exclusion Record**
* NEW! Added new properties ‘Site IDs’ and ‘Group IDs’ in the action and align action results. (TIPG-3609)
* **Create Hash Exclusion Record**
* NEW! NEW action for creating a hash exclusion for a white list. (TIPG-3608)
* **Mitigate Threat**
* NEW! NEW action for applying a mitigation action to a group of threats. (TIPG-3610)
* **Mark As Threat**
* NEW! NEW action for marking suspicious threats as a threat. (TIPG-3612)
* **Resolve Threat**
* NEW! NEW action for resolving threats. (TIPG-3611)
* **Get Threats**
* NEW! NEW action for getting threats list. (TIPG-3613)
* **ServiceNow**
* **CreateRecord**
* Added JSON Result to action "Create Record". (TIPG-3440)
* **Slack**
* **WaitForReply**
* Fixed a bug, where action wouldn't execute even with proper parameters. (TIPG-3702)

**Connectors:**

* **EmailV2**
* **Generic IMAP Email Connector**
* Fixed a bug in marking email as read functionality that caused the connector to fail with Fastmail provider. (TIPG-2861)
* **FireEyeHX**
* **FireEye HX Alerts Connector**
* NEW! FireEye HX alerts Siemplify connector added. (TIPG-3383)
* **QRadar**
* **Qradar Correlation Events Connector V2**
* Fixed bug QRadar offense partially matched events are missing. (TIPG-3631)