RSA Archer GRC

RSA Archer Security Operations Management 1.3

Customization Options for RSA Security Analytics Incident Management Data Flow through RSA Archer Security Operations Management

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers:
http://www.emc.com/support/rsa/index.htm.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November 2015

Contents

Document Revision History

Date	Revision
November 2015	Initial Creation

Preface

About This Guide

This document lists different customization options for Security Analytics Incident Management Data flow in RSA® Archer Security Operations Management.

The audience for this document is the RSA Archer administrator.

RSA Archer Documentation

You can access the RSA Archer documentation from the RSA Archer Exchange and RSA Archer Community.

Documentation	Location
Platform	On the RSA Archer Community at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer**
Solutions, Applications, and Content	On Content tab on the RSA Archer Exchange at: **https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange**

RSA continues to assess and improve the documentation. Check the RSA Archer Community and RSA Archer Exchange for the latest documentation.

RSA Security Analytics Documentation

For information about RSA Security Analytics, see the following documentation:

Guide	Description
RSA Security Analytics Help	The RSA Security Analytics Help provides information needed to understand and use RSA Security Analytics features. It contains topics and tutorials to help you learn the basics of the user interface, system configuration, and analysis concepts. In addition, troubleshooting information for common situations is added on a continuous basis.

You can access this reference material from the RSA Security Analytics Unified Dashboard.

RSA Archer Security Operations Management Data Dictionary

The RSA Archer Security Operations Management *Data Dictionary* contains configuration information for the solution.

You can obtain the *Data Dictionary* for the solution by contacting your RSA Archer Account Representative or calling 1-888-539-EGRC.

Support and Service

Customer Support Information	**www.emc.com/support/rsa/index.htm**
Customer Support E-mail	**archersupport@rsa.com**

Other Resources

RSA Archer Community enables collaboration among GRC clients, partners, and product experts. Members actively share ideas, vote for product enhancements, and discuss trends that help guide the RSA Archer product roadmap.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer

RSA Archer Exchange is an online marketplace dedicated to supporting GRC initiatives that delivers on-demand applications with service, content, and integration providers to drive the success of RSA Archer clients.
https://community.emc.com/community/connect/grc_ecosystem/rsa_archer_exchange

RSA Solution Gallery provides information about third-party hardware and software products that have been certified to work with RSA products. The gallery includes Secured by RSA Implementation Guides with instructions and other information about interoperation of RSA products with these third-party products.
https://gallery.emc.com/community/marketplace/

RSA SecurCare Online (SCOL) provides unlimited access to a wealth of resources on the Web, 24 hours a day. The secure system provides members access to a support knowledgebase, to download current platform patches and bug fixes, to sign up for notifications, to manage your support cases and more.
https://knowledge.rsasecurity.com/

Purpose

There are several ways to customize RSA Security Analytics Incident Management module (SA IM) to suit a particular customer's environment. For example, if a customer has a specific method for tagging users or machines, or an MSSP wants to tag particular customers, additional alert or event attributes can be added and used in rules to automatically create incidents. Also, Incidents can be categorized with additional threat categories.

When these incidents are pushed to RSA Archer Security Operations Management for executing the Incident response, Remediation response, or Breach response workflows, the additional alert and event attributes can be made visible in RSA Archer Security Operations Management enabling L1/L2 incident handlers effectively investigate and remediate the incidents.

The RSA Unified Collector Framework (UCF) integrates SA IM with RSA Archer Security Operations Management. This document serves the purpose of documenting the different customization options that can be enabled for end to end data flow from SA IM to RSA Archer Security Operations Management through UCF.

Scope

The alert/event enrichment happens at the core RSA Security Analytics (SA) devices level and source component level, such as SA Event Stream Analysis (ESA), SA Reporting Engine (RE), SA Malware Analysis (MA), and RSA Enterprise Compromise Assessment Tool (ECAT). There is no post-alert enrichment available in Incident Management. This document's scope doesn't include the alert enrichment from core SA devices and source component level.

The scope of this document is confined to enabling the customization options in SA IM, UCF and RSA Archer Security Operations Management.

Supportability

This document supports the following versions of the products:

- RSA Security Analytics 10.4.1.1, 10.5 or later
- RSA Archer Security Operations Management 1.3
- RSA Archer GRC Platform 5.4 SP1 or later

Use Case Examples

The following use-cases are provided as examples to guide you through the process of adding and mapping the new attributes and categories.

Use Case 1 (UC1) - Include a New "Event_Level" Attribute for events part of ESA and RE Alerts

- UC1 - Step 1 - Include a New EVENT Attribute "Event_Level" for ESA Alerts in SA IM
- UC1 - Step 2 - Group by Event Meta "Event_Level" – (Optional)

Include Additional Alert and Event attributes

Include additional attributes in Security Analytics Incident Management Alerts and Events

New Event Meta from Security Analytics (SA) Core Devices and Components

The starting point for all Alert customization is in the various features used to add attributes to events coming from the core SA devices. Customizing events using feeds, parsers, ESA-named windows and other features is out of the scope of this document. Because ESA and RE alerts are just groups of NextGen events (with ESA optionally adding additional enrichment attributes), the event data is the source for all upstream customization.

The alert and event enrichment happens at the core SA devices level and source component level (ESA, RE, MA and ECAT). There is no post-Alert enrichment available in Incident Management.

Important: SA IM must be enabled to process the additional Meta coming from alerts and events. To include the additional Meta, do the following:

- Edit the alert normalization scripts to normalize the additional Meta.
- Optionally, aggregate the alerts into Incidents with the new alert/event Meta added.

Alert Normalization - Include the Additional Meta

To bring event attributes into the normalized Alert format, edit one of the scripts defined in /opt/rsa/im/scripts/normalize. These scripts are written in JavaScript using the embedded Rhino scripting engine, which implements features of JavaScript 1.8. Any of the changes you make to these scripts take effect within a minute of saving the script file. These are intentionally designed to be updated at runtime in the customer environment.

Additional Meta can be included for ESA, RE, MA and ECAT alerts. The respective scripts below need to be updated to include the additional Meta.

The following table describes the scripts.

Script	Used for	Description
normalize_alerts.js	Defining which script to use	The dispatcher that includes other scripts and makes decisions of which specific script should be used to normalize the incoming Alert. Unless you're adding a new Alert source or one of the sources starts identifying its product name differently, you'll rarely have to change this file.
normalize_core_alerts.js	SA Event Stream Analysis (ESA), SA Reporting Engine (RE) Alerts	Translates Alerts that contain events from one of the "core" nextgen appliances - i.e. Reporting Engine and ESA alerts, pseudo-Alerts created as part of creating an Incident directly from the SA Investigator view, and the "meta" portion of Malware Analysis alerts that were the result of files found in a network session.
normalize_ma_alerts.js	SA Malware Analysis (MA) Alerts	Translates Alerts from MA.
normalize_ecat_alerts.js	RSA ECAT Alerts	Translates Alerts from the RSA Enterprise Compromise Assessment Tool (ECAT).
utils.js	Utility functions	Various utility functions to work around the different ways each product encodes certain data types, or rolling up unique values.

These scripts take the attributes from the original events or the Alert header and copy them to some predictable attribute name in the normalized Alert. In some cases, a concept does not directly translate into the Alert format needed to show data in a consistent way, so unique values are derived, 1 to many or many to many relationships are flatted out, etc. The one-to-many nature of Alerts to Events is not always conducive to displaying a simple grid with the same types of values for every Alert (e.g. there is not just one "source" device if an ESA alert represents 20 events from different sources).

UC1 - Step 1 - Include a New EVENT Attribute "Event_Level" for ESA and RE Alerts in SA IM

Procedure

1. SSH to the SA Webserver host.
2. Edit the java script file normalize_core_alerts.js located in opt/rsa/im/scripts/normalize on the SA web server.
3. In the generateEventInfo function, map the "event_level" field in the normalizedEvent variable, as follows:

```
event_level: Utils.stringValue(event.event_level)
```

Examples for more event attributes below:

```
category: Utils.stringValue(event.category),
action: Utils.stringValue(event.action),
event_source: Utils.stringValue(event.event_source),
level: Utils.intValue(event.level),
did: Utils.stringValue(event.did),
risk_info: Utils.stringValue(event.risk_info),
risk_warning: Utils.stringValue(event.risk_warning),
risk_suspicious: Utils.stringValue(event.risk_
suspicious),
client: Utils.stringValue(event.client),
threat_source : Utils.stringValue(event.threat_source),
threat_desc : Utils.stringValue(event.threat_desc),
service : Utils.stringValue(event.service)
```

4. Save the file.
   Note: The changes take into effect within a minute of saving the script file. Any new ESA Alerts having event_level attribute get normalized properly with the new Meta.
5. The event_level value can be viewed from the "View Event Details" action for the corresponding event in the alert details page in SA IM.
   - To navigate - go to SA UI, click Incidents >Alerts.
   - Choose the alert from ESA and double click on it to go into the Alert details page
   - Click Actions > View Event Details

UC2 - Step 1 - Include a New ALERT Attribute "Threat_Info" for ESA and RE Alerts in SA IM

Procedure

1. SSH to the SA Webserver host.
2. Edit the java script file normalize_core_alerts.js located in opt/rsa/im/scripts/normalize on the SA web server.

3. In the normalizeAlert function, map the "threat_info" field (the assumption here is that threat_info is coming in the alert header from ESA alerts):

```
normalized.threat_info = headers.threat_info;
```

4. Save the file.
   Note: The changes take effect within a minute of saving the script file. Any new ESA Alerts having threat_info get normalized properly with the new Meta.
5. Threat_info value won't be displayed on the SA IM UI, but will be normalized and stored in the ALERTS collection in the MongoDB and will be forwarded to RSA Archer Security Operations Management.

Aggregate the alerts group by new alert/event attributes

Group by a New Alert Attribute

Once a new attribute has been captured as part of the normalization script, it remains in the database in the Alerts collection as the "alert" attribute in each document. Because MongoDB has a flexible schema, all attributes added to the Alert is available to query against in rules.

You can use the advanced mode in the Alert rule builder to construct a MongoDB query that matches against the new attribute you added. You can also customize the attributes that are available in Query Builder to make it easier to build rules that use the new attributes. Find the alert_rule.json file in the /opt/rsa/im/fields/ folder. This file is designed to be updated at run-time in the customer environment.

The following table shows the description of the alert attributes.

Attribute	Description
value	Field from the normalized alert.
name	Name in the UI.
type	"textfield","datefield", "numberfield", "combobox"
groupBy	True if the field should also appear in the "Group By" section of the rule builder. Multi-valued fields are currently excluded due to some limitations in how the rule builder constructs the query.
operators	Corresponds to an index.

The following table shows how the index corresponds to operators.

Index	Operator
0	is equal to
1	is not equal to
2	is greater than
3	is equal or greater than
4	is less than
5	is equal or less than
6	older than

7	newer than
8	begins with
9	ends with
10	contains
11	matches regex
12	in
13	not in

UC2 - (Optional) Step 2 - Group by Alert Meta "Threat_Info"

Procedure

1. SSH to the SA Webserver host.
2. Edit the alert_rule.json file located at opt/rsa/im/fields on the SA web server.
   Add the newly added event attribute to the group by meta list, append this at the end of the file:

```
{
        "value": "alert.threat_info",
        "name": "Threat Info",
        "type": "textfield",
        "operators": [0, 1, 8, 9, 10, 11, 12, 13],
        "groupBy": true
}
```

3. Save the file.
   Note: The changes take effect within a minute of saving the file.
4. The newly added field is shown in the Group by options list in the Aggregation Rules in Security Analytics Incident Management. To Navigate:
   - On SA UI, click Incidents > Configure > Aggregation Rules.
   - Create a new Rule or Edit existing rule to group by the new Meta and enable the rule.

Group by a new Event attribute

Group by some of the event Meta like source IP address, destination IP address was added as part of the SA IM 10.4.1.1, 10.5 releases.

To include the newly added event meta in the group by clause in the rules, add attributes to the Alert data by editing the normalize_alerts.js script located at /opt/rsa/im/scripts/normalize. Add extra filters to the rule builder by editing alert_rules.json located at /opt/rsa/im/fields by following the procedure in UC1 - (Optional) Step 2 - Group by Event Meta "Event_Level".

UC1 - (Optional) Step 2 - Group by Event Meta "Event_Level"

Procedure

1. SSH to the SA Webserver host.
2. Edit the java script file normalize_alerts.js located in opt/rsa/im/scripts/normalize on the SA web server.

3. In the normalizeAlert function, include the newly added event meta in the "else" section. This generates flattened column values for group by fields that can have multiple values.

```
normalized.groupby_event_level = Utils.generateFlattenedColumnValue(normalized.event_level);
```

4. Save the file.
5. Edit the alert_rule.json file located at opt/rsa/im/fields on the SA web server.
6. Add the newly added event attribute to the group by meta list, append this at the end of the file:

```
, {
    "value": "alert.events.event_level",
    "name": "Event Level",
    "type": "textfield",
    "operators": [0, 1, 8, 9, 10, 11, 12, 13],
    "groupBy": true,
    "groupByField": "alert.groupby_event_level"
}
```

7. Save the file
   Note: The changes take into effect within a minute of saving the file.
8. The newly added field is shown in the Group by options list in the Aggregation Rules in Security Analytics Incident Management.
   - To Navigate: On SA UI, click Incidents > Configure > Aggregation Rules.
   - Create a new Rule or Edit existing rule to group by the new Meta and enable the rule.

Add the additional Meta for Alerts and Events in RSA Archer Security Operations Management

In RSA Archer Security Operations Management, applications can be customized to include additional fields and displayed according to the layout specifications. For adding a new field to the security events application, edit the Security Events application, add a new field and include it in the layout for Security Events application. The Security Alerts application can be customized to include the additional Meta.

View GUIDs for New Fields

GUIDs are needed to map the new fields from Archer to SAIM in the UCF mapping file. Through the API code generated for the corresponding application, users can get the GUID for the newly added field.

UC1 - Step 3 - Add a New "Event_Level" Attribute to Security Events Application in Archer Security Operations Management

Procedure

1. In RSA Archer GRC UI, go to Administration > Manage Applications > Security Events > Fields > Add New.
2. Click the 'Copy an existing field radio button, and choose a field with a Text Field Type.
3. Change the Name to "Event Level", the Alias to Event_Level, and choose a Description for the field.
4. Click Save.

5. Click on the Layout tab for the Security Events application.
6. Drag the new field you created on to the layout to the intended location.
7. Click Save.
8. To get the GUID for the newly created field, go to Administration > Integration > Obtain API Resources > Generate API Code.
9. Select the Security Events application.
10. Click Download the Source File.
11. In the source file, look for "Event_Level" field. Take a note of the GUID for the newly added field. For example, the GUID is b925bf52-cf19-451e-b429-19d655543790 from the below code.

```
/// <summary>
/// Event Level
/// </summary>
public static readonly Guid Event_Level = new Guid("b925bf52-cf19-451e-b429-19d655543790");
```

UC2 - Step 3 - Add a New "Threat_Info" Attribute to Security Alerts in RSA Archer Security Operations Management

Procedure

1. In RSA Archer GRC UI, Go to Administration > Manage Applications > Security Alerts > Fields > Add New.
2. Click the Copy an existing field radio button, and select a Text field.
3. Change the following information:
    - Name to "Threat Info".
    - Alias to "Threat_Info".
4. Choose a Description for the field.
5. Click Save.
6. Click the Layout tab for the Security Alerts application.
7. Drag the new field you created on to the layout to the intended location.
8. Click Save.
9. To get the GUID for the newly created field, go to Administration > Integration > Obtain API Resources > Generate API Code.
10. Select the Security Alerts application.
11. Click Download the Source File.
12. In the source file, look for "Threat_Info" field. Take a note of the GUID for the newly added field and field type.

For example, the GUID is b70dfbcc-d2db-46a7-9511-722be3cef06a from the below code.

```
/// <summary>
/// Threat Info
/// </summary>
public static readonly Guid Threat_Info = new Guid("b70dfbcc-d2db-46a7-9511-722be3cef06a");
```

Map the additional Alert/ Event Meta from SA IM to Archer in UCF mapping file

After adding the additional fields to Alerts and Events in SA IM and RSA Archer Security Operations Management, the newly added fields must be mapped in the UCF. The secops_import_archer.xml file is used to map the fields from SA IM to RSA Archer Security Operations Management. This file is located in the <install_dir>\config\mapping folder on the machine where UCF is installed.

Alert and Event Mappings related to the following different Applications are present in the secops_import_archer.xml file. Customize the respective application to map the additional fields from SA IM to Archer Security Operations Management. Updates to this file require restart of the RSA Unified Collector Framework Service.

The following table shows the application and mode that should be used.

Application	**Scenario**	**Description**
SecurityIncident_Security Events	Security Events part of the Security Incidents	SecOps mode - if the mode is chosen to manage the incident workflow exclusively in RSA Archer Security Operations Management. All the incidents created in SA IM (along with alerts and events part of them) are forwarded to RSA Archer Security Operations Management. In that case, UCF uses this mapping to map the fields part of Security events.
SecurityIncident_Security Alerts	Security Alerts part of the Security Incidents	SecOps mode - if the mode is chosen to manage the incident workflow exclusively in RSA Archer Security Operations Management. All the incidents created in SA IM (along with the alerts and events part of them) are forwarded to RSA Archer Security Operations Management. In that case, UCF uses this mapping to map the fields part of the Security Alerts.
DataBreach_Security Events	Security Events part of the Data Breaches	Non-SecOps mode - if chosen to manage the incident workflow in RSA Security Analytics. Data Breaches created in SA IM (along with the incidents, alerts and events part of them) will be forwarded to RSA Archer Security Operations Management. In that case, UCF uses this mapping to map the fields part of the Security Events.
DataBreach_Security Alerts	Security Alerts part of the Data Breaches	Non-SecOps mode -if chosen to manage the incident workflow in RSA Security Analytics. Data Breaches created in SA IM (along with the incidents, alerts and events part of them) will be forwarded to RSA

		Archer Security Operations Management. In that case, UCF uses this mapping to map the fields part of Security Alerts.
Findings_Security Events	Security Events part of the findings	Non-SecOps mode - if chosen to manage the incident workflow in RSA Security Analytics. Remediation tasks assigned to GRC/ Operations queue created in SA IM (along with the incidents, alerts and events part of them) can be forwarded to RSA Archer Security Operations Management as Findings. In that case, UCF uses this mapping file to map the fields part of Security Events.
Findings_Security Alerts	Security Alerts part of the findings	Non-SecOps mode - if chosen to manage the incident workflow in RSA Security Analytics. Remediation tasks assigned to GRC/ Operations queue created in SA IM (along with the incidents, alerts and events part of them) can be forwarded to RSA Archer Security Operations Management as Findings. In that case, UCF uses this mapping file to map the fields part of Security Alerts.

For the respective application, map the new fields in the following format:

```
<field name="Name of Archer field that needs to be mapped">
        <UUID>GUID from Archer</UUID>
        <fieldType>Type of field</fieldType>
        <keyName>relative JSON path of the field</keyName>
</field>
```

The following table shows the fields that need to be mapped.

Field Name	**Element**	**Description**
Field Name	Name of the field that is being mapped	Field name from RSA Archer Security Operations Management.
UUID	GUID from Archer	GUID from Archer. The GUID that we retrieved from the API code for the new field added.

fieldType	Type of Field	Can be any of the following: 1. CROSS_REFERENCE 2. RELATED_RECORD 3. DATE 4. NUMERIC 5. TEXT 6. TRACKING_ID 7. VALUES_LIST 8. IP_ADDRESS 9. EXTERNAL_LINK
keyName	Relative JSON Path of the Field coming from SA IM	Contains relative JSON path and not absolute path where only the immediate parent node (should be one of incident/alerts/events) should be defined. Example: For mapping the Source IP address, the relative JSON path from the events node is events.source.device.ip_address.

UC1 - Step 4 - Map the New "Event_Level" Attribute in the UCF

Procedure

1. Log on to the machine on which RSA Unified Collector Framework is installed.
2. Open secops_import_archer.xml, located in <*Install_Dir*>\SA IM integration Service\config\mapping.
3. Add the following code to the SecurityIncident_Security Events application:

```
<field name="Event Level">
      <UUID>b925bf52-cf19-451e-b429-19d655543790</UUID>
                  <fieldType>TEXT</fieldType>
                  <keyName>event.event_level</keyName>
</field>
```

   Note: UUID is the GUID obtained from Step 3. keyName is the relative JSON path for the field from SA IM.

4. Save the mapping file.
5. Restart the RSA Unified Collector Framework Service from Control Panel > Administrative Tools > Services.

UC2 - Step 4 - Map the New "Threat_Info" Attribute in UCF

Procedure

1. Log on to the machine on which RSA Unified Collector Framework is installed.
2. Open secops_import_archer.xml, located in the <*Install_Dir*>\SA IM integration Service\config\mapping folder.
3. Add the following code to the SecurityIncident_Security Alerts application:

```
<field name="Threat Info">
        <UUID>b70dfbcc-d2db-46a7-9511-722be3cef06a</UUID>
        <fieldType>TEXT</fieldType>
        <keyName>alerts.threat_info</keyName>
</field>
```

Note: UUID is the GUID obtained from Step 3. keyName is the relative JSON path for the field from SA IM.

4. Save the mapping file.
5. Restart the RSA Unified Collector Framework Service from Control Panel > Administrative Tools > Services.

Add, Edit or Remove Threat Categories for Security Incidents

Additional values can be added to the threat categories for incidents. For example, Customers might need to categorize their incidents based on their sites. Or to add any new threat categories that their organization requires. To add the additional threat categories for incidents, we need to add the new categories in SA IM, Archer and map them in UCF mapping file.

Customize Threat categories for Incidents in Security Analytics Incident Management

The Incident Categories are loaded the first time the IM service runs on a new database server in the "categories" collection. The out-of-the-box Categories are based on the "Action Enumerations" in VERIS framework. Each document is a specific sub-category, containing an "_id" (auto-generated by MongoDb), "parent" for the general type of category (e.g. "Malware"), and "name" for the name of the sub-category. Incidents are associated with zero or more specific entries in this collection.

For including additional categories, new documents needs to be added as part of the "Categories" collection with a parent and child category defined. Adding this automatically takes into effect without restarting the IM service.

UC3 - Step 1 - Add the new Parent and Child Threat Categories for incidents in SA IM

Procedure

1. Connect to the IM database by logging onto the Mongo shell on the database host.
   IM Database is configured to use ESA host, in general. To get the host of the server where IM is hosted, follow the steps below:

   - Click Administration > Services on SA UI.
   - Choose Incident Management Service, click Actions > View > Explore.
   - In the left hand side panel, choose Service > Configuration > Database
   - Look for the defined Hostname or IP Address.

2. SSH to the IM Database host, type “mongo”:

```
[root@SA-server ~]# mongo
```

3. Run the following commands to add a category called "STRIDE" with two sub-categories, "Spoofing" and "Tampering", as follows:

```
> use im
switched to db im
> db.categories.insert( {"parent": "STRIDE", "name": "Spoofing"})
> db.categories.insert( {"parent": "STRIDE", "name": "Tampering"})
```

4. To add a new sub-category JSON Injection to the existing Hacking parent category,

```
> db.categories.insert( {"parent": "Hacking", "name": "JSON Injection"})
```

Note: The changes take into effect within a minute.

5. The new category with the sub-categories is listed in the categories dropdown in SA IM UI.
   - To navigate on SA UI, Click Incidents > Queue > 'All Incidents'
   - Choose any of the incidents, Click 'Edit' icon.
   - In the Categories dropdown, verify that new categories are displayed.

UC4 - Step 1 - Edit/ Remove existing Threat Categories in SA IM

1. Connect to the IM database by logging onto the Mongo shell on the database host.
   IM Database is configured to use ESA host, in general. To get the host of the server where IM is hosted, follow the steps below:
   - Click Administration > Services on SA UI.
   - Choose Incident Management Service, click Actions > View > Explore.
   - In the left hand side panel, choose Service > Configuration > Database
   - Look for the defined Hostname or IP Address.

2. SSH to the IM Database host, type "mongo":

```
[root@SA-server ~]# mongo
```

3. Run the following command to move a sub-category from one parent to another parent category:

```
> use im
switched to db im
> db.categories.update({"parent": "<old_parent>", "name": "<sub-category>"}, { $set: {"parent":
"<new_parent>"}})
```

4. Run the following command to edit the sub-category name :

```
> db.categories.update({"parent": "<parent_category>", "name": "<old_name>"}, { $set: {"name":
"<new_name>"}})
```

5. Run the following commands to remove the entire parent category:

```
> db.categories.remove({"parent": "<parent-category>"})
```

6. Run the following commands to remove only the sub-category:

```
> db.categories.remove({"parent": "<parent-category>", "name": "<sub-category>"})
```

Note: The changes take into effect within a minute.

7. The category changes can be observed in the Categories dropdown in SA IM UI.
    - To navigate on SA UI, Click Incidents > Queue > 'All Incidents'
    - Choose any of the incidents, Click 'Edit' icon.
    - In the Categories dropdown, verify that categories changes are reflected.

Customize threat categories for Incidents in RSA Archer Security Operations Management

Threat Categories is a value-list containing parent and child categories and is part of the Security Incidents application in RSA Archer Security Operations Management. New parent or child categories can be added to the existing values.

UC3 - Step 2 - Add the New Parent and Child Categories in RSA Archer Security Operations Management

Procedure

1. In RSA Archer GRC UI, Go to Administration > Manage Applications > Security Incidents > Fields.
2. Select the Threat Category field.
3. On the Values tab, click Add New.
4. Enter Stride in the Text Value field.
5. Click Save.
6. Add the two sub-categories, Spoofing and Tampering, Drag and drop each sub-category under the Stride parent category.
7. Add a new "JSON Injection" category. Drag and Drop the sub-category under the Hacking category.
8. Click Save.
9. To get the GUID for the newly created fields, go to Administration > Integration > Obtain API Resources > Generate API Code.
10. Select the Security Incidents application.
11. Click Download the Source File
12. In the source file, look for all the three newly added categories (1 parent category and 3 sub-categories). Take a note of the GUIDs for those newly added categories.
13. For example, this is the GUID for the STRIDE category: 9a977505-0ae6-42e0-bead-c40cf6b73955

```
/// <summary>
/// Stride
/// </summary>
public static readonly Guid Stride = new Guid("9a977505-0ae6-42e0-bead-c40cf6b73955");
/// <summary>
/// Spoofing
/// </summary>
public static readonly Guid Spoofing = new Guid("422bc135-1018-465a-a0ca-0d5218c85f6b");
/// <summary>
/// Tampering
/// </summary>
public static readonly Guid Tampering = new Guid("9b8e2ace-d5ba-48d4-91b2-ba75ef931c0f");
```

```
/// <summary>
/// JSON Injection
/// </summary>
public static readonly Guid JSON_Injection = new Guid("2429ad44-33ec-495d-9e59-35eff7e52c5a");
```

UC4 - Step 2 - Edit/ Remove existing categories in RSA Archer Security Operations Management

Procedure

1. In RSA Archer GRC UI, Go to Administration > Manage Applications > Security Incidents > Fields.
2. Select the Threat Category field.
3. To Edit, On the Values tab - choose the category/ sub-category that you would like to edit.
4. Edit the "Text Value" for the field.
5. Click Save.
6. To Delete, On the Values tab - choose the category/ sub-category that you would like to delete.
7. Click Delete.
8. Click Save.

Map the threat categories from SA IM to Archer in UCF mapping file

After adding the additional categories to incidents in RSA Archer Security Operations Management, the new fields added should be mapped in UCF. secops_import_archer.xml file is used to map the fields from SA IM to RSA Archer Security Operations Management. This file is located at <install_dir>\config\mapping folder in the machine where UCF is installed.

Incident mappings related to the following different Applications are present in secops_import_archer.xml file. Customize the respective application to map the additional fields from SA IM to RSA Archer Security Operations Management. Updates to this file require restarting the RSA Unified Collector Framework Service.

The following table shows the application that should be used. If you would like to include the new category for all security incidents, it needs to be mapped in all of the below applications.

Application	Scenario	Description
SecurityIncident	Security Incidents	SecOps mode - if the mode is chosen to manage the incident workflow exclusively in RSA Archer Security Operations Management. All the incidents created in SA IM (along with alerts and events part of them) are forwarded to RSA Archer Security Operations Management. In that case, UCF uses this to map the fields for Security Incidents.
DataBreach_Security Incident	Security Incidents part of DataBreach	Non-SecOps mode - if the mode is chosen to manage the incident workflow in RSA Security Analytics. Data Breaches created in SA IM (along

		with the incidents, alerts and events part of them) will be forwarded to RSA Archer Security Operations Management. In that case, UCF uses this to map the fields for Security Incidents.
Findings_Security Incident	Security Incidents part of the findings	Non-SecOps mode - if the mode chosen to manage the incident workflow in RSA Security Analytics. Remediation tasks assigned to GRC/ Operations queue created in SA IM (along with the incidents, alerts and events part of them) can be forwarded to RSA Archer Security Operations Management as Findings. In that case, UCF uses this to map the fields for Security Incidents.

UC3 - Step 3 - Map the Additional Parent and Child Threat Categories in the UCF

Procedure

1. Log on to the machine on which RSA Unified Collector Framework is installed.
2. Open secops_import_archer.xml, located in the <*Install_Dir*>\SA IM integration Service\config\mapping folder.
3. Append the mapping for the newly added values to the Security Incident application in the Threat Category values list.

```
<field name="Threat Category">
<UUID>d36656d6-cbec-4b30-b8bc-7fce058461e5</UUID>
   <fieldType>VALUES_LIST</fieldType>
   <keyName>incident.categories</keyName>
   <valueFieldUUIDs><!-- Stride-->
          <valueFieldUUID name="Stride">9a977505-0ae6-42e0-bead-c40cf6b73955</valueFieldUUID>
          <valueFieldUUID name="Stride:Spoofing">422bc135-1018-465a-a0ca-0d5218c85f6b</valueFieldUUID>
          <valueFieldUUID name="Stride:Tampering">9b8e2ace-d5ba-48d4-91b2-ba75ef931c0f</valueFieldUUID>

   <!All the other categories follow>
```

   Note: UUIDs are the GUID values obtained from Step 2.

4. If the parent category already exists, map the sub-category under the existing category. See below:

```
 <valueFieldUUID name="Hacking">f99ccd6b-2518-40c6-b410-196545027a59</valueFieldUUID>
   <valueFieldUUID name="Hacking:JSON Injection">2429ad44-33ec-495d-9e59- 35eff7e52c5a</valueFieldUUID>

<!All the other categories follow>
```

   Note: UUIDs are the GUID values obtained from Step 2.

5. Save the mapping file.
6. Restart the RSA Unified Collector Framework Service from Control Panel > Administrative Tools > Services.

UC4 - Step 3 - Edit/ Delete the existing mapping from UCF Mapping file

Procedure

1. Log on to the machine on which RSA Unified Collector Framework is installed.
2. Open secops_import_archer.xml**,** located in the <*Install_Dir*>\SA IM integration Service\config\mapping folder.
3. To edit the existing threat category, in the Security Incident - look for the corresponding threat categories mapping and change the sub-category to a new sub-category.

```
<valueFieldUUID name="<parent_category>">f99ccd6b-2518-40c6-b410-196545027a59</valueFieldUUID>
<valueFieldUUID name="<edited_category_name>"><same_guid_as_before></valueFieldUUID>
```

4. To remove the existing threat category, in the Security Incident Application – remove the existing mapping for the category.
5. Save the mapping file.
6. Restart the RSA Unified Collector Framework Service from Control Panel > Administrative Tools > Services.