Rsam SSRS Report Installation Requirements and Administration Guide

SIRP Executive Report

Document Version: 2017.01 | August 2017

Contents

About this Guide

Each Rsam SSRS report has a unique set of steps for installing the report and ensuring that all the required configurations for the report are met. This guide provides a walk through of all the items to consider when installing the **SIRP Executive Report** and executing it for the first time.

For general information about integrating SSRS with your Rsam environment, refer the document *RSAM Reporting - SSRS Integration*.

For information on building your own SSRS reports, refer the document *Rsam Platform Step-by-Step Tutorial - Building SSRS Reports*.

Overview

This guide provides details around the installation artifacts and configuration dependencies required to run the SIRP Executive Report.

Minimum Rsam Version

The minimum version of Rsam required to execute this report is **9.2.2126.2**.

Required Modules

This report requires that you have licensed and installed the **SIRP** baseline module.

Required SSRS Artifacts

This section provides information about the required SSRS artifacts for the SIRP Executive report.

Report-Specific SSRS Artifacts

The following Report Definition Language files and Stored Procedures must be applied in your Rsam environment.

If your Rsam instance is on premise, then add the RDL files to your report server using SSRS Report Manager.

If your Rsam instance is in the Rsam Cloud, then contact support to have the RDL files added to your environment.

Report Definition Language (RDL) Files

The following Report Definition Language files must be applied in your Rsam environment.

RDL File Name	Description
SIRP Executive Report.rdl	This is the primary RDL file for the SIRP Executive Report.
SIRP_SubReport_SecurityEvents.rdl	This is the RDL file for the SIRP Security Events sub report.
SIRP_SubReport_SecurityIncidents.rdl	This is the RDL file for the SIRP Security Incidents sub report.

Stored Procedures

The following stored procedures must be applied in your Rsam environment. These procedures are included in the file called **SIRP Executive Report – Stored Procedures.sql**, which is included in the report installation package.

If your Rsam instance is on premise, have a database administrator execute this script against your database.

If your Rsam instance is hosted in the Rsam Cloud, please work with Rsam Support to have this script applied to your Rsam database.

Stored Procedure Name	Description
rpt_Get_IncidentRelated_Hosts	Fetches the data required for the "Top 5 Hosts by Incident Count" chart.
rpt_Get_EventRelated_Hosts	Fetches the data required for the "Top 5 Hosts by Event Count" chart.

Configuration Dependencies

Before executing the report, you must ensure that your Rsam environment includes all the configuration elements on which the report depends. This section details the searches, record types, attribute types, and other elements that must be available in the environment before executing the report. New Rsam customers will have these items included in the databases by default, but existing customers who want to add SSRS reports to their existing Rsam environments may need to obtain these items from Rsam in the form of environment migration files.

Attribute Types

The record attribute types listed in the following table must be present in your Rsam environment for the report to execute successfully. They are available in optional environment migration script called **SIRP Executive Report – Attributes.**

Note: If you are an existing Rsam customer, applying these attribute types to your environment through an environment migration script may overwrite configuration changes that you have made to those attribute types.

Record Type Admin Name	Rsam ID
SIRP: Event Category	RSAMR9-00002144-A6CC8EE5E9A74916812749971C27446F"
SIRP: Date Created	RSAMR9-00002159-07DF1EEED1CE484A9324322878900405
SIRP: Related Hosts	RSAMR9-00002157-AF04A07AAFEE46ECA743ED22AF7149C7
SIRP: Incident Category	RSAMR9-00002326-5721FB498B2144F690D29D009C311D2E
SIRP: Incident State	RSAMR9-00002324-8C3A4AD044904B3B823FB33F7CE214D2
SIRP: Incident Country	RSAMR9-00002326-5721FB498B2144F690D29D009C311D2E
U: Open / Closed	RSAM01-00000861-033032A0D51F4743A243FBA49B4B70C2

Searches

A set of searches must be present in your Rsam environment for the report to execute successfully. These searches have been created specifically for use with the SSRS report (note the naming convention). These searches should not be modified for use within other parts of Rsam (navigators, charts, etc.). If you want to use these searches throughout other areas of Rsam, it is recommended that you create copies of these searches and modify the searches for the required purposes.

The following table lists the searches that must be present in your Rsam environment for the SIRP Executive Report to execute successfully. To add these searches to your environment, import the environment migration script, **SIRP Executive Report - Searches**.

Search Name	Rsam ID
SIRP: Events by Workflow State (SSRS)	RSAMA6-00003645-321F2C1C0D7C4ED1945457D94FBE3DDF
SIRP: Events by Category (SSRS)	RSAMA6-00003649-7E5F3D23774A4FC3B8848B18C0D287D8
SIRP: Incidents by Workflow State (SSRS)	RSAMA6-00003647-5C18271D57B84F899AF273E5E11C255E
SIRP: Incidents by Month (SSRS)	RSAMA6-00003653-AC79E6CBA5D541BA9725BD96B5F0EE3C
SIRP: Incidents by Location State (chart) (SSRS)	RSAMA6-00003655-6100994F475E4B74AA89C62DE075B107
SIRP: Incidents by Location Country (chart) (SSRS)	RSAMA6-00003657-6D9605877D374A9FB8C0C5BDF11B2E4E
SIRP: Incidents by Category (SSRS)	RSAMA6-00003651-E4465DD03CD7445AAE70D183C3A7DBAC

Record Types and Record Category Types

The record types and record category types mentioned in the following tables are included as part of the SIRP baseline module in Rsam and for most customers. These serve as the record types that are presented in the SIRP Executive Report.

If you have created custom event or incident record types, those will be included in the report if the following criteria are met:

- You have included your custom record category types in the SSRS-specific searches
- You have associated your record types with the required attribute types

Note: If you are an existing Rsam customer, applying these record types to your environment through an environment migration script may overwrite configuration changes that you have made to those record types.

The following table lists the Record Types for the SIRP Executive report.

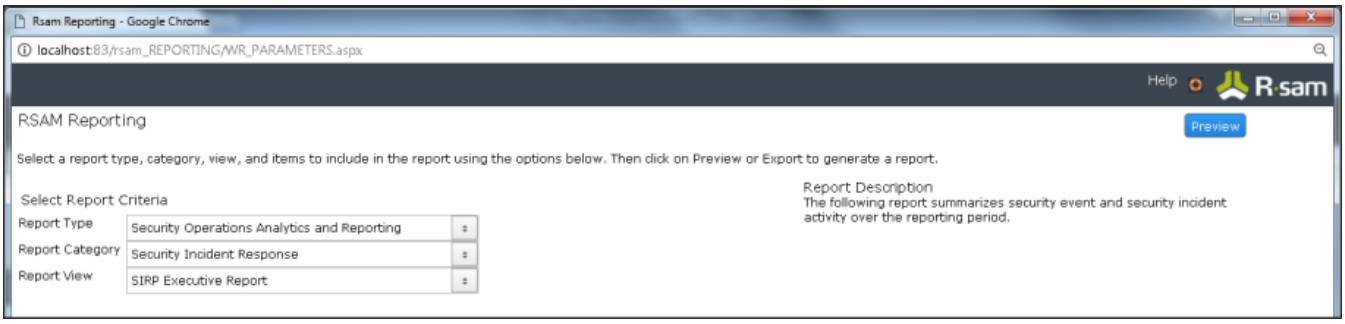
Record Type Admin Name	Rsam ID
SIRP: Checkpoint Event	RSAMR9-00000545-D4425B8AE5B44E7AA76C4C700BACC871
SIRP: AWS Event	RSAMR9-00000544-CF6764094BCB4F098D7C50D9AEC7FEBE
SIRP: Splunk Event	RSAMR9-00000541-D9BAEA6A594947AE9E95CBF46F4B8A83
SIRP: QRadar Event	RSAMR9-00000540-E988FEA4698A4D9DAB775E2FF547E885
SIRP: ArcSight Event	RSAMR9-00000539-389A1DB91BC54B50BF88F06CD45CFE82
SIRP: Event	RSAMR9-00000522-FB390982131E450C90AB894AE5F762E9
SIRP: Incident	RSAMR9-00000523-60672CDD89B342EDBC183AC4BA406027
SIRP: Symantec Endpoint Protection	RSAMR9-00000625-8D4751B666A2434FBDFAAA43DFABD134

The following table lists the Record Category Types for the SIRP Executive Report.

Record Category Type Admin Name	Rsam ID
SIRP: SIRP Incident	RSAMR9-00000448-FDCE1984B11E41DF85B57A3BB9FAF8CD
SIRP: SIRP Event	RSAMR9-00000449-68E0A5DBC6344DAAB2E197ADD6240AD2
SIRP: SIRP - ArcSight	RSAMR9-00000460-C1614E4AA6694410935C9B66E41E062C
SIRP: SIRP -QRadar	RSAMR9-00000461-7A5A1E851717449988213FA0ACE6DE88
SIRP: SIRP - Splunk	RSAMR9-00000462-7250F69C3A5D467EB5F84498CE259903
SIRP: SIRP - AWS	RSAMR9-00000465-755D6E63E5504617BA974E3D7DBF71F3
SIRP: SIRP - Checkpoint	RSAMR9-00000466-E0E4CBE7DC0F48A4993C413C19F8ABBF
SIRP: SIRP - Symantec Endpoint Protection	RSAMR9-00000518-682F365C8A914FB489175E6E0B4D4BDE

Report Record

To access the report from the **Reports** menu in Rsam, you must apply the report record through the provided migration script - **SIRP Executive Report – Report.**



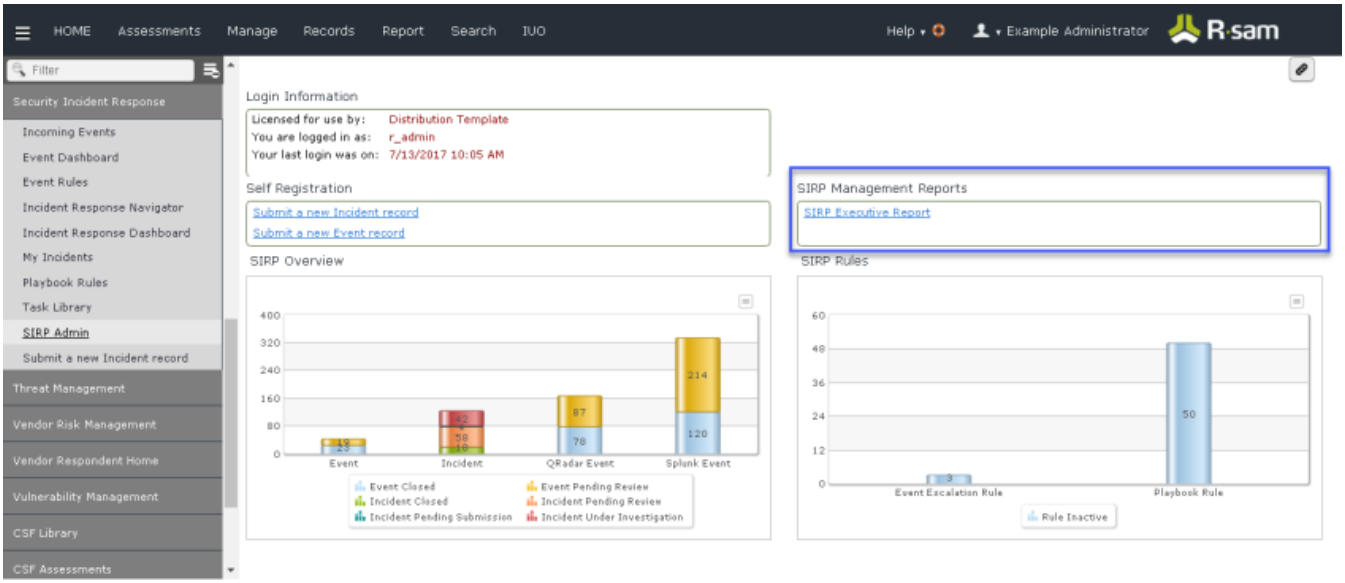
The following table lists the name and ID of the report.

Record Name	Rsam ID
SIRP Executive Report	RSAMA6-00000240-C68864CE20AE4C5895E7C6538E9CF41D
Security Operations Analytics and Reporting (Report Type)	RSAMA6-00000236-2560462764F949BFBA6371E575CB0E84
Security Incident Response (Report Category)	RSAMA6-00000239-0F81A8B6264D4A52ABA0ABE04BFFD7E1

Home Pages

In addition to the **Report** menu, the SIRP Executive Report can be accessed also by adding a link to view the report, to any home page. If you want to include a link in your environment, add it to any home page by placing a **Report List widget type** on that home page tab.

The following image shows an example home page tab with a Report List widget type, which includes a link to open the SIRP Executive report.


HOME
Assessments
Manage
Records
Report
Search
IUO
Help
Example Administrator
Filter
Security Incident Response
Incoming Events
Event Dashboard
Event Rules
Incident Response Navigator
Incident Response Dashboard
My Incidents
Playbook Rules
Task Library
SIRP Admin
Submit a new Incident record
Threat Management
Vendor Risk Management
Vendor Respondent Home
Vulnerability Management
CSF Library
CSF Assessments
Login Information
Licensed for use by: Distribution Template
You are logged in as: r_admin
Your last login was on: 7/13/2017 10:05 AM
Self Registration
Submit a new Incident record
Submit a new Event record
SIRP Management Reports
SIRP Executive Report
SIRP Overview
SIRP Rules
Event
Incident
QRadar Event
Splunk Event
Event Closed
Incident Closed
Incident Pending Submission
Event Pending Review
Incident Pending Review
Incident Under Investigation
Event Escalation Rule
Playbook Rule
Rule Inactive

Using and Managing your Report

This section of the guide explains a unique or advanced feature of this specific SSRS report. The feature mentioned in this section is intended for report administrators who might require a deeper understanding of how the report functions in order to maintain the report over time.

Report Prompts

The SIRP Executive Report provides a global filter for determining the reporting period. All event and incident data will be filtered to show only those items that have a **SIRP: Date Created** value that falls within the selected reporting period. If you do not see any data returned in your report, expand this date range to include a wider time period.