Security Analytics: Risk and Visibility Report

The Risk and Visibility Report in Security Analytics is a powerful way to provide non-analysts, executives, and other members of your organization with a general overview of the latest threats that have been detected by Security Analytics. It's also a great way to track progress as you make improvements on your network to fortify security. The report gives you a high-level view and reports including:

- The predicted count of files hiding in encrypted traffic. Modern day threats are hiding in encrypted traffic
- The amount of encrypted traffic crossing your network. Might be enlightening to you.
- Risky applications on the network. Do you know what applications are in use across your network?
- Anomalous network behavior based on a benchmark of your actual traffic. Identify what "normal" is in your network so you can identify "abnormal".
- An executive summary to share with security team or management so you can prioritize activities. It's a great way to shine light on the value of Security Analytics.

Getting the report is quite easy:

> The logged-in user must be in a group that has permission to generate the report under *Menu* ☰ > *Analyze* > *Reports* in the permissions table.
>
> If you import a PCAP, pivot to the *Summary* page, and then run the *Risk and Visibility* report for the PCAP, you should add a few minutes to the timespan so that data-enrichment verdicts can be included in the report.

1. Select ***[Account Name]***  ***> Risk and Visibility Report***.
2. Select the desired timespan. By default, the timespan in the current window is selected.
3. Select one or both options:
   - **Email** — In the space provided, specify one or more comma-delimited email addresses. For this option, you must also specify an email server on *Menu* ☰ > *Settings* > *Communication* > *Server Settings* > *Email Settings*.
   - **Download** — A PDF of the report is generated. When it is finished, you can download it from the system notifications.
4. You can monitor the progress of the report by selecting **Menu** ☰ **> Analyze > Report Status > List**. The reports are displayed with **Risk Report** in the **Name** column. To stop the *Risk and Visibility* report, select the check boxes for all of the reports and click **Delete**.

Report Status

Delete

	ID	Username	Field	Timespan Start	Timespan End	Start	End	Processing Time	Name	Saved	Disk Usage	State	Actions
	6787	admin	url_risk_verdict	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:08		00:16:55.493315	Risk Report	false	32 kB	active	
	6786	admin	file_signature_verdict	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:08		00:16:55.51607	Risk Report	false	32 kB	active	
	6785	admin	malware_analysis_verdict	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:08		00:16:55.529077	Risk Report	false	16 kB	active	
	6784	admin	ipv4_responder	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:08		00:16:55.636422	Risk Report	false	16 kB	active	
	6783	admin	application_group	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:08	06/01/2017 11:41:36	00:00:28	Risk Report	false	32 kB	complete	
	6781	admin	ipv4_responder	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:07		00:16:56.167931	Risk Report	false	16 kB	active	
	6780	admin	ipv4_initiator	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:07		00:16:56.176423	Risk Report	false	16 kB	active	
	6779	admin	ipv4_responder	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:07		00:16:56.213021	Risk Report	false	16 kB	active	
	6778	admin	ipv4_initiator	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:07		00:16:56.216302	Risk Report	false	16 kB	active	
	6777	admin	ipv4_initiator	05/16/2017 12:14:27	05/16/2017 12:20:33	06/01/2017 11:41:07		00:16:56.222193	Risk Report	false	16 kB	active	

Here's what you'll see in the Risk & Visibility Report: (Get a sample copy here)