Implementing risk-based alerting

With Splunk Enterprise Security, you use the traditional approach of alerting on narrowly-defined detections that are often reactive to the current trends in attack methods. As a security analyst, you would like to have more tangible, actionable alerts with much higher fidelity.

This article is part of Splunk's Use Case Explorer for Security, which is designed to help you identify and implement prescriptive use cases that drive incremental business value. In the Security maturity journey described in the Use Case Explorer, this article is part of Alert prioritization.

Implement risk-based alerting

Risk-based alerting (RBA) provides teams with a unique opportunity to pivot resources from traditionally reactive functions to proactive functions in the SOC. As alert fidelity and true positive rates increase, analysts' resources can be shifted to higher impact tasks like threat hunting or adversary simulation, empowering SOCs to build up the skill sets of their analysts and prepare them for any threats they might encounter.

The RBA methodology is very similar to what you are likely already doing in Splunk Enterprise Security. It uses nearly all of the existing frameworks within Splunk Enterprise Security but includes a few optimizations that dramatically increase efficiencies and general security maturity within the SOC.

The benefits of RBA include:

- a dramatic reduction in the overall alert volume (alert fatigue)
- improved detections
- alignment with popular frameworks such a MITRE ATT&CK
- more detections and data sources without scaling up SOC operational costs
- increased detection time ranges
- a more streamlined deployment process

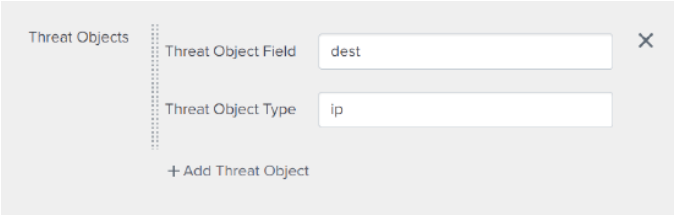
Key features

The frameworks in Splunk Enterprise Security version 6.4 and later provide out-of-the-box features for implementing RBA. You can leverage the Risk Analysis adaptive response action and assign risks to multiple unique risk objects within a rule. Additionally, you can use the modular input for MITRE ATT&CK, which links Risk Rules to corresponding MITRE ATT&CK technique IDs through CSE (Risk Annotations). All corresponding MITRE context is stamped into the event.

- Annotation Framework
    - Use annotations to enrich your correlation search results with the context from industry-standard cyber security framework mappings

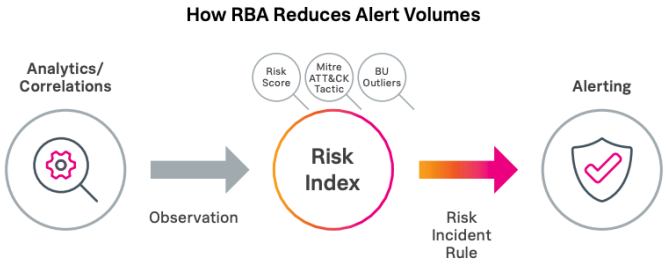
- Risk Analysis Adaptive Response Action
  - Added flexibility when attributing context to risk objects
  - Improved integrations with the Asset & Identity framework
  - Stored lookup that adds the additional MITRE ATT&CK context based on the technique
- Risk Factoring Framework
  - Provides the ability to modify the risk score up/down based on field values in the risk index
  - Usually based on asset/identity info but can operate on fields like “action”, “priority”, “category”, etc.
  - Applied when events are inserted into the Risk Analysis data model
- Threat Objects (Patent Pending)
  - Allow you to associate possible Indicators of Compromise (IOC) with an analytic
  - Creates a new vector in security that allows you to understand “behavior” from an IOC perspective
  - Lowers the barrier for localized threat hunting
  - Aids in the Investigative process
  - Allows you to attach many possible IOCs to the notables that get sent to Splunk SOAR

By using the Threat Objects feature in your Risk Rules, you can build a local repository of Indicators of Compromise (IoC) or Indicators of Behavior (IoB). This threat data is extremely important due to its high relevance to investigative, threat intelligence, and especially threat hunting activities within the SOC.



How to implement RBA

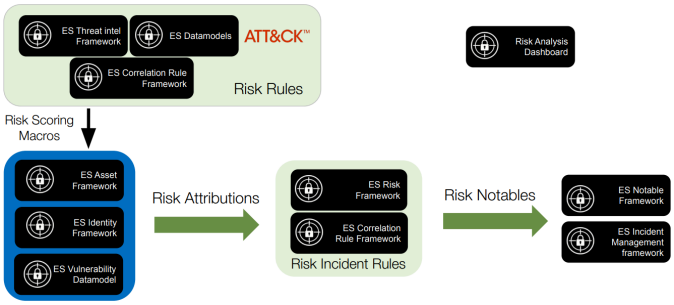
RBA works by using the existing Splunk Enterprise Security correlation rule framework to collect interesting and potentially risky events and put them together in a single index from which to alert. When these events are collected in the Risk Index, it then produces a single Risk Notable only when certain criteria are met. This increases the fidelity of alerts that SOC team members must review, thus reducing the time and workload of analysts.



The following are the components that make RBA work. They are part of the continuous workflow of creating and developing your RBA maturity. These components can be summarized into five categories:

- Risk Rules & Notables
  - Risk Rules add events to the Risk index
  - Risk Notables are created by the risk incident rules
- Risk Scoring
  - Initial scoring of assets & identities
- Risk Modification
  - Risk is updated by risk factors & ad-hoc risk changes
- Risk Attribution
  - Enhanced by MITRE tactics & techniques
- Visualizations & Workflow
  - Analysts use dashboards & workflows to work through the high fidelity risk notables

RBA Risk Rules can be sourced from the collection of out-of-the-box Splunk Enterprise Security rules from ES Content Updates (ESCU) or Splunk Security Essentials (SSE).

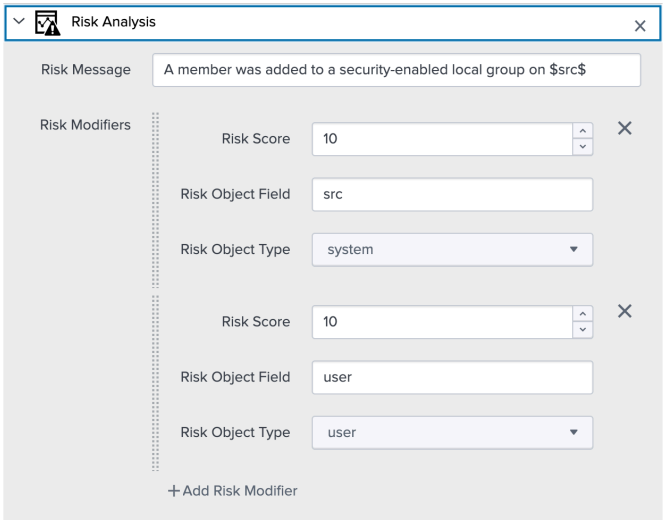


The following steps will guide you through getting started with enabling support for the RBA methodology within your Splunk Enterprise Security environment.

1. **Modify existing correlation searches in ES**.
   a. **Add MITRE ATT&CK technique.** In the top navigation bar in Splunk Enterprise Security, click **Configure** > **Content** > **Content Management**, then filter by Type=**Correlation Search**. Select the correlation search you would like to modify and locate the annotations section. Refer to the Mitre Att&ck matrix and locate the technique or subtechnique that best aligns with your CS. Type the technique number into the annotations.

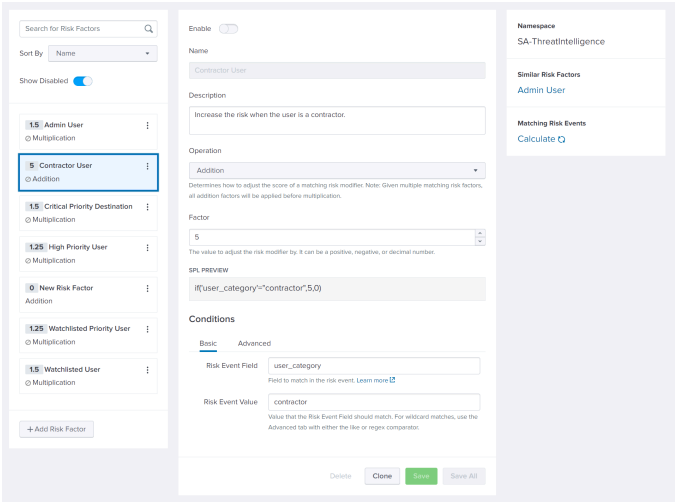
   b. **Add a risk analysis adaptive response action.** In your query, you will often have multiple entities. An entity

can be any user/device field such as username, ip addresses, hostnames, etc. Most often these will be fields like src, dest, or user. There can be multiple risk modifiers, so ensure that each entity in your search query is represented. This example will create two risk entries, one for src and one for user.

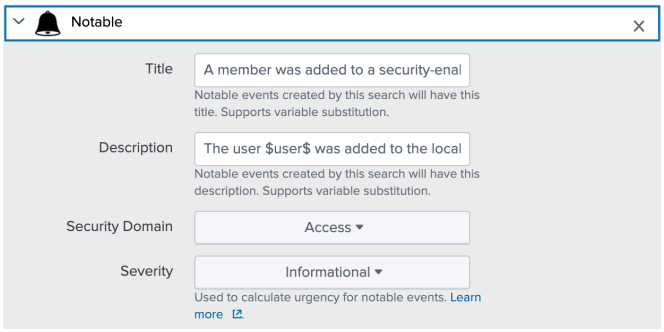


If you don't know what risk score to use, consider using the same value for everything such as 10 unless you have a reason to do otherwise.

c. The Risk Factor Editor allows for fine-tuning of Risk Scores based on organizational- and environmental-specific policies. This context enables a true *Risk* informed triage and analysis of observed behavior. For example, in the following screenshot, we have added five (5) to the risk score whenever a user is categorized as a Contractor as they present additional risk due to different personnel security controls. By using Risk Factors effectively, you can be sure you're pointing your analysts to the most important events based on your organization's needs.



d. **Determine the alert action.** Finally, it is entirely optional as to whether you want to keep the notable alert action. One suggestion is to create "Informational" notables so you can still investigate them in the incident review page.



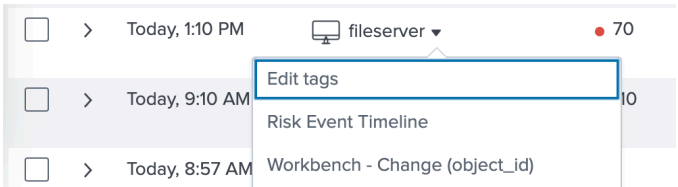
2. **Start searching the risk index.** After you have developed a baseline of risk data, search the risk index (index = risk). This will help you become familiar with the data and annotations that are building.
Also consider ways you could work with this data. For example:
    - Look at the risk_object field. How can you see if more than one MITRE technique has occurred for any given value?
    - How can I add up the risk scores for each risk_object?
    - Over what timespan does the analysis make the most sense? Should I analyze 7 day windows, 31 days, etc?
3. **Enable the built-in aggregation rules.** There are two correlation searches included in ES that are designed to create risk notables.

The “ATT&CK Tactic Threshold Exceeded” detection looks for risk objects that have seen multiple attack techniques over a 7 day window. Consider changing the “where” clause to make it more or less sensitive. For example: `| where mitre_tactic_id_count >= 2 and source_count >= 2`

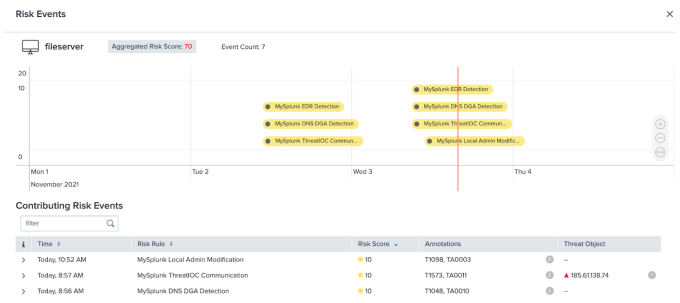
On a similar note, look at the “Risk Threshold Exceeded” detection and consider what changes to make. One suggestion is to change it to a longer timespan to help find low-and-slow attacks. Also adjust the risk threshold as needed.

4. **Update the incident review settings.** In the ES Incident Review page, you should now see the “Risk notables” type when the above alerts trigger.

You will also be able to view the risk event timeline from the risk object.



This timeline provides a powerful view in order to begin an investigation and visualize all risk events.



If you have been using Splunk Enterprise Security for a while and have previously customized the incident review settings, you may not see these new columns. To add those back in, go to **Configure** > **Incident Management** > **Incident Review Settings**. Review the columns you have and consider adding back in any fields below that you might need.

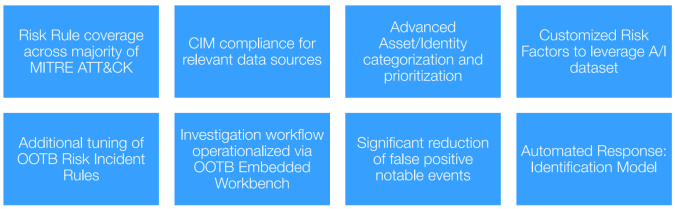
That's it! Now you can start going through additional correlation searches and performing the same steps to add more context into the risk index. If you get stuck, use the MITRE ATT&CK framework or the Splunk Security Essentials app to discover new behaviors that are of value to your team.

RBA milestones

The following milestones show what the progression may look like as you mature in your RBA implementation. These steps can be used to guide you through maturing your implementation with the goal of getting to the highest level of automation and analytics.

Level 1: Proof of Concept

Level 2: Use Case Expansion



Level 3: Additional Context, Performance Management

Level 4: Automated Response, Advanced Analytics

Next steps

For a comprehensive RBA demo and workshop, or to engage Professional Services for setting up RBA in your environment, reach out to your Splunk account team or representative. In addition, these Splunk resources might help you understand and implement this use case:

- YouTube How-To: Risk Based Alerting: The new frontier for SIEM
- .Conf Talk: Supercharge your risk-based alerting (RBA) implementation
- .Conf Talk: Building behavioral detections: Cross-correlating suspicious activity with the MITRE ATT&CK framework
- .Conf Talk: Modernize and mature your SOC with risk-based alerting
- .Conf Talk: Getting started with risk-based alerting and MITRE
- .Conf Talk: Tales from a threat team: Lessons and strategies for succeeding with a risk-based approach
- .Conf Talk: Full speed ahead with risk-based alerting (RBA)
- .Conf Talk: Streamlining analysis of security stories with risk-based alerting
- Docs: Isolate threats with risk alerting
- Webcast: Curing alert fatigue with risk-based alerting, MITRE ATT&CK and automation