Overview
In a modern day SOC, dealing with alert fatigue is a real problem. It will often lead to overburdened analysts, situational numbness, and ultimately, true positive detections will go overlooked. Whether you have a small, moderate, or large security analyst team, this model of security monitoring is time consuming, and difficult to scale. As an alternative method for incident response with the Enterprise Security premium application, Splunk has created a risk-based approach to security monitoring called Risk Based Alerting (“RBA”). Bundle the RBA offering with your Enterprise Security Implementation Success offering for reduction of noisy alerts, improved detections, and increased security maturity.

One of the key differentiators of RBA is the fact that it actually provides a high-level view of an overall threat activity, by associating related but potentially malicious alerts and combining them into a single risk-based event. This provides an analyst with a more comprehensive view of the overall activities associated with a threat actor. Most traditional security tools provide an alert based upon a single activity group. This means that an analyst typically misses the relationship between related acts or threats, that could be associated with the campaign for example, at the moment of being notified of the first event. It is typically only discovered later in the incident triage process. By leveraging the power of RBA, activities that relate to an overall attack, can be connected and reported on in a single event. This means that an analyst is now able to respond with an attack associated with a threat source, as opposed to individual events.

One of the common complaints from the security operations at this is the lack of visibility. This visibility can be from the perspective of not receiving alerts and can also occur when an analyst is not able to see the full threat activity landscape and respond appropriately. Beyond the initial response is also the need to enrich the initial set of data artifacts with additional context from the perspective of external threat intelligence sources, and customer specific information such as prior user activity, or adding additional information related to the threat. By combining RBA with Phantom, we provide the analyst with a comprehensive data rich view, and provide them the options to triage further or launch a set of responses to defeat the attacker, at the push of a button.

RBA Maturity Model
Splunk Professional Services will work closely with the customer to define their RBA maturity model over time, based on customer capabilities and best practices seen in the field.

Offering Highlights
This service delivery offering is designed to launch a customer on the journey to enable them to leverage the RBA to accelerate the maturity of their security operations model. It provides the necessary knowledge transfer workshops and the development of the RBA model, with the corresponding response models inside Splunk Phantom (if applicable). The outcome of this engagement is a trained empowered customer team that can evolve and mature their risk models, enabling them to gain great visibility, enhance event correlation and faster response.

Offering Description
Every customer is different, so we have built three different RBA implementation success approaches to provide flexibility to different customer needs. Each of our offerings will bring the customer to a full RBA framework implementation, varying levels of data sources, risk rules, alerting, and risk modifiers.

Options to Fit Your Needs
The objective of this engagement is to enable the customer to develop, manage and evolve the RBA model to meet their current and future needs, and develop the corresponding response models, leveraging their instance of Phantom.
**Designed to Meet Your Needs**

This offering is designed for customers with more internal resources dedicated to the Splunk project. Internal Splunk Admins and Users will receive informal training from the Splunk Accredited Consultant and will complete tasks remaining after Splunk Professional Services finishes their work.

<table>
<thead>
<tr>
<th>Workshop</th>
<th>RBA Enablement</th>
<th>Phantom Response Model Tuning (Optional)</th>
<th>Total Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 days</td>
<td>8 days</td>
<td>+10 days</td>
<td>10-20 days</td>
</tr>
</tbody>
</table>

**Components Included**

<table>
<thead>
<tr>
<th>RBA Workshop and Documentation</th>
<th>Risk Rules</th>
<th>Risk Notables</th>
<th>Risk Modifiers</th>
<th>Dashboards</th>
<th>OAR Response Workbooks (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>10</td>
<td>2</td>
<td>5 modifiers using existing A/I framework</td>
<td>2 (Investigative risk attribution dashboards)</td>
<td>Investigative Enrichment</td>
</tr>
</tbody>
</table>

Additional components (risk rules, risk incident rules, modifiers, asset/identity customization, additional response workbooks, etc.) beyond the initial offering can be added on an a la carte basis, and estimated time will be adjusted accordingly. See optional add-ons below.

**Optional Add-Ons**

- **Add Additional Risk Incident Rule(s)**
  The purpose of this add-on is to co-develop a RiR to produce risk based alerts. The outcome of this work is a RiR triggering Risk Notable Events, based up to 5 Risk Rules, and 3 Risk Modifiers. The work product generated by this add-on is an additional Risk Incident Rule that can be deployed in production.

- **Additional Risk Rules** (10 in 5 days)

- **Risk Modifiers: Add a Framework**
  (5 day per framework)
  Splunk co-develops the creation of new risk modifiers and integrates a new framework, with the goal of enabling the customer to continue the development and fine tuning of the risk modifiers and frameworks to meet their unique needs.

- **Risk Incident Rule Tuning** (Custom time)
  This optional add-on engages Splunk Risk experts to review your existing Risk Incident Rules, Risk Notables and Risk Modifiers with the goals of tuning and improving the efficiency and effectiveness of RBA.

- **Add an OAR Response Model**

- **On-Demand Services**
  Additional dashboards/customizations, SPL help, etc.

**How to Engage**

For assistance, contact your Splunk Account Manager. They can coordinate with Professional Services to assist you with sizing the migration. Visit our website at [www.splunk.com](http://www.splunk.com) or email [cs-sales@splunk.com](mailto:cs-sales@splunk.com) for help getting started.

**Splunk Professional Services**

We exist to get customers to valuable outcomes with their data – faster than they could on their own. Our services are backed by Splunk Accredited Consultants, Architects, and Delivery Managers. They leverage Splunk best practices and experience from thousands of Splunk deployments.