Splunk RBA Implementation Success

Professional Services

Optimize for the alerts that matter

Taking advantage of risk-based alerting (RBA), through Splunk Enterprise Security, will greatly empower and maximize the efficiency of your SOC. Splunk's RBA Implementation Success offering allows you to successfully deploy, adopt and realize value faster with standardized risk and risk incident rules as the foundation to building a more resilient enterprise with Splunk. If you are already leveraging Splunk Security Orchestration, Automation and Response (SOAR) or in the process of implementing it, Splunk has developed a Risk Notable Playbook Pack, to be deployed with Splunk SOAR, specifically tailored to enrich and triage alerts generated through the RBA methodology, allowing your team to work smarter and respond faster to alerts.

Successful implementation of risk-based alerting can yield the following target results:[1]

- Reduce alert volume by up to 50% to 90%
- Greatly minimize false positives
- Reduce mean time to detection / recovery

Key benefits

- Launch a full RBA framework implementation within Splunk Enterprise Security, with varying levels of data sources, risk rules, alerting, risk modifiers, maturity, and SOAR functionality leveraging a pre-built Risk Notable Playbook Pack (if applicable).
- Accelerate time to value by tapping into our implementation experience and delivery methodology.
- Build deep technical expertise on your team through knowledge transfer and enablement.

1 Results dependent on package size, customer commitment & resources, and implementation complexity.

Service at a Glance	
Best for	New and existing customers using Enterprise Security seeking to implement RBA with standard best practice risk and risk incident rules.
Duration	10-20 days (depending on option selected: Base or Standard, details below)
Prerequisites	**ES Version 6.6+ installed** • Splunk deployment in a healthy state for critical assets • Data Fully Onboarded and CIM Compliant • Data Models tuned according to best practices • Assets and Identities Framework in place (Strongly recommended) • Vulnerability data onboarded (Optional, but recommended) • RBA Champion identified **SOAR (if applicable)** • SOAR previously provisioned and installed/configured • Customer incident response SOPs include community supported SOAR integrations
Project Team	Splunk Solutions Architect Splunk Certified Consultant
Deliverables	• RBA workshop and discovery • Build & Configure risk incident rules • Configured risk and risk incident rules • Risk modifier framework • RBA maturity roadmap • RBA operational runbooks • Knowledge Transfer with security team • Implement and configure SOAR Risk Notable Playbook Pack (if applicable)

What we'll do and deliver

Discover and Design

Kickoff to align on goals, do technical discovery and conduct a deep-dive planning workshop to understand your technical environment and risk profile.

Build and Configure

Define and build a framework for risk and risk incident rules based on the threat environment and create a tailored roadmap to mature your security posture rapidly.

Knowledge Transfer

Deliver a maturity roadmap readout for stakeholders and conduct a knowledge transfer session with your security team.

Resilience, let's build it together

Splunk Customer Success provides end-to-end success capabilities at every step of your journey to accelerate time to value, optimize your solutions and discover new capabilities. We offer professional services, education and training, customer success management, and technical support, surrounding you with the expertise, guidance and self-service success resources needed to drive the right outcomes for your business.

For more information visit **splunk.com/askcs**, or email us at **cs-sales@splunk.com** to connect.

Implementation details

Phase	Tasks	Base	Standard
RBA Planning Session	• RBA Workshop and Discovery	1 day	1 day
RBA Implementation	• Implement identified components • Create Risk Rules • Create Risk Incident Rules • Create Risk Modifier Framework • Out-of-the-box functionality only	8 days	13 days
RBA Enablement & Knowledge Transfer	• Conduct knowledge transfer on implemented components • Guidance on RBA maturity	1 day	1 day
SOAR Risk Notable Playbook (optional)	• Implementation of SOAR risk notable playbook pack • Limited to 1 functional use case (Investigate, Response, or Recover) • 3 community supported integrations	+5 days, if applicable	+5 days, if applicable

Terms and Conditions:

This Solution Guide is for informational purposes only. The services described in this datasheet are governed by the applicable fully signed ordering document and any incorporated terms and conditions.

24-324651-Splunk RBA Implementation Success Services Datasheet-103-A