GUIDEPOINT SECURITY
GOVERNMENT SOLUTIONS

SPLUNK RISK-BASED ALERTING QUICKSTART SERVICES

Enhance Your SOC's Ability to Detect and Respond to Alerts in a Dynamic Security Environment

Further mature your SOC through Risk Based Alerting to mitigate alert fatigue and produce more true positives.

The Risk Based Alerting (RBA) model can provide great benefits to your security team, but can be complicated to set up. We can help you get RBA setup in your environment quickly and improve the effectiveness of your security operations.

Traditionally, alerts generated are triaged one at a time, which quickly causes alert fatigue in your SOC as your organization grows. You also run into increased false positives, forcing your analysts to create multiple whitelists, suppressions, and spend valuable time tuning searches, all which can create potential blind spots in your security.

Running RBA inside Splunk Enterprise Security (ES) can fix these issues. When something suspicious happens, instead of generating an alert, the attributions are written to a Risk Index. You can also enrich the data in your Risk Index by assigning risk scores, a relevant MITRE ATT&CK tactic and technique, and also classifying if a user or asset is related to a Business Critical Application or Department. Next, a notable event is triggered if a user or asset crosses a predetermined risk score threshold or specific patterns of behavior.

What are the Benefits of RBA?

Enhanced Detection

- Discover sophisticated APTs and "low and slow" attacks that are difficult to detect in current environments.

Proactive Security

- Evolve from a reactive to proactive SOC to detect and respond to attacks in near real time.

Cyber Security Framework

- Align with your favorite security framework like MITRE ATT&CK, NIST, Lockheed Martin Cyber Kill Chain and many more.

Ability to Expand to Detect Insider Threat

- RBA is capable of detecting suspicious activity from within an organization and employees exfiltrating intellectual property and sensitive documents.

Put a Highly-Trained ELITE Team on Your Side

Our highly-certified, operational cybersecurity experts have lived and breathed your job.

- More than **70%** of ourworkforce consists of tenured cybersecurity engineers, architects and consultants
- Many have managed security within the DoD and U.S. intelligence agencies and **Fortune 500 companies**

Leverage Our Splunk Expertise

Supported Quickstart RBA Assessment

Our RBA Quickstart Service checks your Splunk Enterprise Security environment and conducts an assessment of the following items:

- Data feeds and CIM compliance
- Assets and Identities Configuration
- Review of Key Searches or Detections
- Data Models
- Inventory of Existing Data and Data not Being Used
- Integration of Ticketing System for Alerts

Focusing on Business Critical Applications and Departments

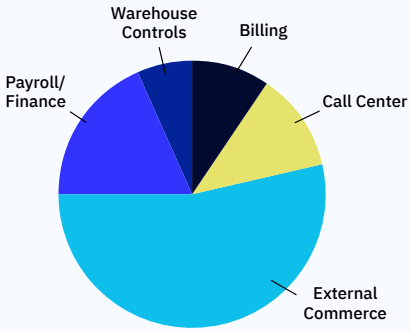
Many organizations have Business Critical Applications and Departments that are at the core of their foundation. Utilize RBA to track each application's risk and also compare risk appetites amongst applications. This allows your organization to go one step further than just looking at users and assets and see trends across departments and even regions!

Business Critical Applications Risk Analysis

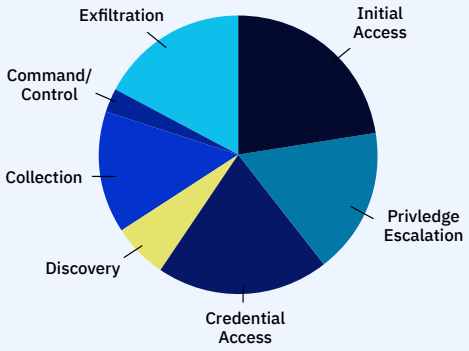
Total Sum Organization Risk Score

272

Risk by Business Critical Application



Risk by MITRE ATT&CK Tactic



Cell Center Department Risk Score	Billing Department Risk Score	External Commerce Department Risk Score	Warehouse Department Risk Score	Payroll/Finance Risk Score
34	25	144	15	54

Quickstart Menu

All Quickstarts include base RBA setup, and the creation of Risk Rules and Risk Notables.

1 Week Quickstart

- Setup RBA
- Create 5 Risk Rules
- Create 2 Risk Notables

2 Week Quickstart

- Setup RBA
- Assess and tune Enterprise Security Assets and Identities
- Create 8 Risk Rules
- Create 2 Risk Notables

4 Week Quickstart

- Setup RBA
- Assess and tune Enterprise Security Assets and Identities
- Create 12 Risk Rules
- Create 2 Risk Notables
- Create 2 Risk Notable Dashboards

GUIDEPOINT SECURITY
GOVERNMENT SOLUTIONS

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
GSA Schedule: GS-35F-508CA | DUNS: 005644870 | SINs 54151S, 54151 HACS