splunk> turn data into doing

Risk Based Alerting Hands-On Workshop

Overview

The Risk-Based Alerting (RBA) hands-on workshop is designed to guide Detection Engineers or other content creators with the RBA process used in Splunk Enterprise Security. Our journey will begin with a review of ES fundamentals as a foundation for RBA then proceeds through Risk Factors, Risk Rule creation, and Risk Notable creation. The workshop leverages the popular Boss of the SOC (BOTS) dataset with hands-on exercises that build on one another and expose the participants to detecting a complex APT attack. The participants will depart with a clear path for getting started with RBA in their environment.

Prerequisite

The Enterprise Security with Risk-Based Alerting Overview and Demo are a required prerequisite for this workshop. This overview is led by SEs, Security SMEs, CSMs, and Specialists and is designed to provide any persona in the SOC with both an understanding of the RBA concept as well as help participants visualize the RBA endgame via a compelling and relevant demo.

Risk-Based Alerting Hands-On

This workshop is led by SEs, Security SMEs, CSMs, and Specialists with advanced cybersecurity knowledge and is designed to give participants hands-on experience with RBA. The lessons learned in this workshop will provide participants with the ability to begin deploying RBA with Enterprise Security. Initial goals include optimizing functions in the SOC such as detection engineering, triage, and investigations which ultimately free up cycles to focus on proactive activities such as adversary simulation, threat intelligence, SOAR, and threat hunting.

The workshop agenda is approximately 4 hours and includes:

- High level overview
- Assets & Identities – Exercise
- MITRE ATT&CK Breakdown – Exercise
- Risk Rule – Exercise
- Risk Incident Rule – Exercise
- RBA and Beyond: Art of the Possible

Workshop Data

The workshop data is sourced from the BOTS v4 2019 data set, focusing on network and host data including:

- Microsoft Sysmon
- Windows Event Logs
- Windows Threat Defender
- Azure Active Directory
- Windows Registry
- Splunk for Stream (Wire Data)

Customers Who Will Benefit

The workshop is designed for personas on a Security Operations team that are responsible for content creation, usually the Detection Engineering team. The workshop has three goals:

1. Walk through Enterprise Security framework terms and components that are leveraged by RBA
2. Understand what components come into play when we start to write detections and operationalize the MITRE ATT&CK framework. Augmenting the traditional Use Case based approach to security with alignment to a popular cybersecurity framework provides quantitative visibility into both current and forward-looking detection, control, and validation strategies.
3. Provide a series of exercises that guides users through the process of setting up RBA including creating a risk rule and enabling other relevant risk rules that ultimately produce that risk notable to streamline the investigative process.

Benefits

- **Expert guidance** from Splunk security subject matter experts: Learn from Splunkers who have years of experience, not only with Splunk products, but also in security. Get your questions answered by people who can relay the value of RBA.
- **Real World Data:** Based on attack scenarios from Splunk's Boss of the SOC, the data collected showcases common security attacks that you may encounter daily. A great deal of care was taken to ensure that the detections built in this lab are real-world relevant while highlighting the benefits of this RBA process.
- **Hands-on Time:** Participants will be exposed to multiple facets of RBA and Enterprise Security. These hands-on-keyboard exercises are designed to answer common questions that appear throughout planning and implementing.

RBA: A First Principle approach to cybersecurity

At Splunk we talk about getting value out of your data, and what we can do with discrete data enriched, analyzed, and acted upon by Enterprise Security. But with RBA, we're bringing even more value out of this data by painting the picture of connected *behavior* which is especially useful in a security context. We do this by building a behavioral layer of abstraction between data and the various functions within the SOC.

Instead of generating single discrete security events in isolation, we are presenting a big picture overview based on potentially connected behaviors. From highly technical analysts to the Executive team, various "stories" can now be discovered or told with behavior across the enterprise, between connected objects, or individual objects.

In addition to utilizing traditional threat intelligence (known threat indicators), we are *creating* custom threat intelligence. It's important to have a vetted list of IPs, domains, and hashes from other environments, but with RBA we're also building a wealth of knowledge about what is normal for our environment. Because we're tracking *behavior* of these assets or user objects, we're also tracking what they're doing or who they're communicating with.

Workshop Logistics

This workshop is hands-on, and each user will need access to a modern web browser with internet connectivity. Splunk will provide a cloud environment where the Splunk software and data will reside.

Splunk Security Strategists

We are here to help customers get the most out of their Splunk deployments. Our services are backed by Splunk experts who provide consistent and quality service delivery, architecture guidance, training, and ongoing support.

Take your Splunk environment to the next level and achieve continual optimization, enhanced processes, and active collaboration. If you are interested in learning more about our workshops as well as BOTS, please contact your Splunk Sales Representative.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.