


SECURITY

Risk-Based Alerting: The New Frontier for SIEM

 By [Haylee Mills](#) April 04, 2022

If you haven't heard the gospel of risk-based alerting (RBA) in a SIEM context, by the end of this sermon you'll see why you'll want it running in your environment yesterday, whether you're an analyst, an engineer, or in leadership.

On a sunny Orlando day in 2018, Jim Agger of Splunk and Stuart McIntosh (now of Outpost Security) delivered a [talk about RBA](#) for Splunk's conf that melted my mind onto a crappy conference room chair. The RBA methodology had been used in other contexts, but for some reason it had not yet been operationalized into a SIEM product where its capabilities could truly shine. With the flexibility of Splunk Processing Language (SPL), their talk showed how it was simply a matter of creating some fields to tie information about objects together, adding security metadata to this information, and wrapping it all together with summary indexing. As of [Splunk Enterprise Security](#) 6.4, RBA is now integrated into correlation searches so you can get up and running as soon as you carve out the time to build the foundation of the framework.

After returning from Orlando, I had new hope for the future of blue teaming. As anyone who is familiar with content engineering knows, you have to spend hours viciously neutering valuable detections as tightly as possible to tune out regular business traffic, and every gap closed by a well-tuned detection is still going to create more analyst busywork. What I saw with RBA was both a solution for alert volume and a way to track complex, interconnected attacker activity that I see all of the cool, mature security teams doing in threat hunts that so many SOC's don't have time for.

When teams are able to carve out the time to build RBA and make the vision a reality, we see so many benefits. Alert volume is regularly reduced by 50-90%, alert fidelity is vastly increased, and we often see red team activity being detected even before RBA is fully in production. There are huge swaths of the MITRE ATT&CK framework that can only be covered by detections which embrace the value in noisy data. Most importantly, the time saved, security maturity capabilities, and operational solutions enabled by RBA prompts a cascade of changes in an organization. I'm usually the first to respond skeptically when a vendor dangles big promises, but RBA is more of a methodology that you customize and build to solve your unique problems. Sometimes when you free one stuck cog, it allows a bunch of other gears to begin moving again.

I plan to post follow-up blogs over the next several weeks to talk about the steps (and potential pitfalls) you might encounter on your RBA journey. But first, I suppose I should answer... what does RBA do for me and what is it, exactly?

What's in it For Me?!

I don't want to sound too hyperbolic, but OMG YOU HAVE NO IDEA I CAN'T WAIT TO TELL YOU SO LIKE IT'S REALLY INCREDIBLE BECAUSE UMM...

Ahem. This is what talking RBA does to me.

So, whoever you are, here is what RBA can do for you.

Leadership

I know you've got a collection of mouths and metrics breathing down your neck so another science project with promises of transformation probably sounds too good to be true. Except this experiment has repeatedly proven wild success. RBA provides:

- A reduction in low-fidelity, time-consuming alert volume. This means more time for high-value activities in your security organization like threat hunting, adversary simulation, and security content development.
- Alignment with cybersecurity frameworks like MITRE ATT&CK, the Lockheed Martin Kill Chain, or CIS20. You can quantify what gaps you are closing, and empower your people to close them faster than ever before.
- The ability to meet and exceed many security audit requirements resulting in a much smoother audit season.

Engineers

There are always a zillion asks, unrealistic vertical or lateral expectations, and barely enough time in the day to work on your pet project that would likely fix a huge gap or inefficiency. I'm telling you... make RBA your pet project. Content development is so much faster when you don't have to endlessly tune and tweak to get low volume, high fidelity alerts. RBA means:

- You can derive value out of noisy security data sources so you can, you'll be able to build all sorts of detections that weren't feasible in the past.
- A flexible risk detection and alerting methodology preventing you from endlessly allowlisting hosts and adjusting logic to try and make alerts that won't overwhelm the SOC.
- You can create zero-risk events that only add risk when seen in conjunction with other behaviors, or only in certain contexts.

Analysts

Just. So. Many. Alerts. Then, having to search multiple sources for other potentially suspicious activity "every time" is a real chore. Having all of that tied together and presented to you automatically means you'll have a much better idea of where to start. With less repetitive alerts you'll have more time to do fun stuff. With RBA:

- Alerts come in with multiple events and more context, providing useful information to make an initial hypothesis for your investigations.
- Threat objects allow you to investigate behaviors and see if something is abnormal for your environment, that business unit, or that user.
- The flexibility of RBA and customization capabilities of SPL mean your feedback is invaluable to develop new features, detections, and quality of life improvements for investigation and response.

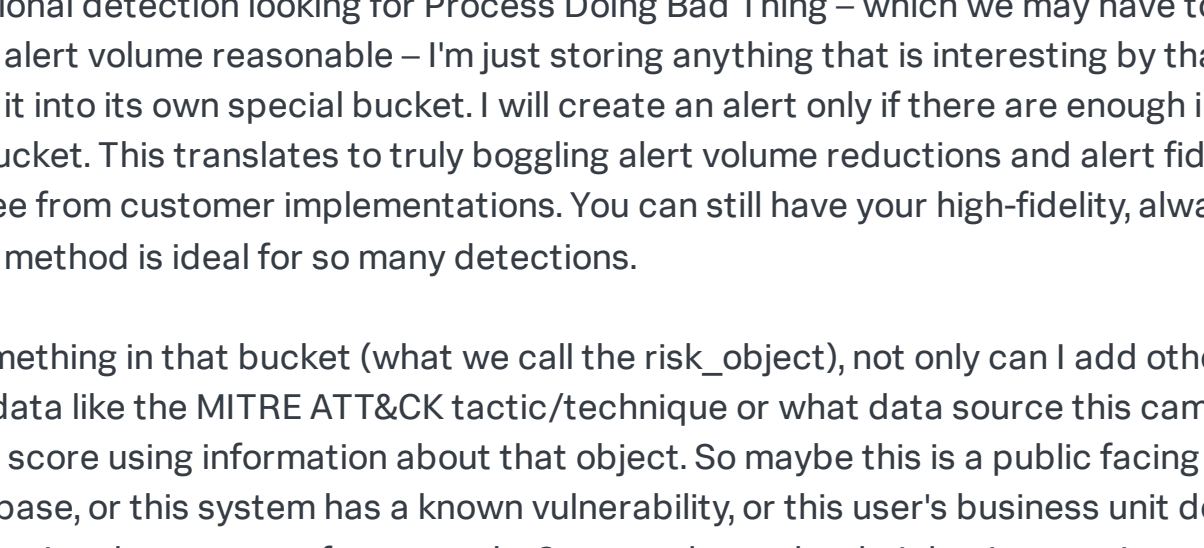
The shift to RBA can seem daunting, but it's a lot easier if we have the right pieces in place to discuss the culture shift with the proper stakeholders. I know everyone's got a lot on their plates, but hopefully this blog will help plant the seed for further discussions. Having discussions with all of the teams involved will keep people on the same (or at least, a similar) page, and each team will have some idea of what might be required of them and more importantly, what problems RBA could help them solve. Likely you will discover some folks who can see the potential and devise solutions to problems you didn't even know your organization had.

What is RBA?

What we're used to with detection is: I have a log source, I write detection logic for some potential badness on that log source, and that detection makes an alert.



With RBA, I like to think that our detection logic provides observations, then we tag that observation with security metadata and tweak the score based on interesting attributes like privileged user, externally facing server, etc. The alert happens only when we have enough interesting observations.



Let's break that down a bit further.

We're all probably familiar with using a score of some kind to indicate a risk's likelihood, severity, or urgency, and that is just one small part of the risk picture. The analogy I like to use is rather than having a flat, unidimensional detection looking for Process Doing Bad Thing – which we may have to spend weeks tuning to keep alert volume reasonable – I'm just storing anything that is interesting by that host, user, or ID and putting it into its own special bucket. I will create an alert only if there are enough interesting things in the bucket. This translates to truly bogging alert volume reductions and alert fidelity increases we regularly see from customer implementations. You can still have your high-fidelity, always-investigate alerts, but this method is ideal for so many detections.

When I put something in that bucket (what we call the risk_object), not only can I add other useful security metadata like the MITRE ATT&CK tactic/technique or what data source this came from, I can also tweak the score using information about that object. So maybe this is a public facing production server or database, or this system has a known vulnerability, or this user's business unit definitely shouldn't be running these types of commands. Conversely, maybe their business unit regularly runs these types of commands and we might tweak that lever in the opposite direction for specific commands. One of my favorite parts of RBA is the creativity we have to add knobs and levers as needed to tweak the way our alerts bubble up without allowlisting. It's always exciting for me to hear about interesting levers people used to solve their specific problems.

In addition, RBA stores the activity or behavior performed by that risk_object as a threat_object. This becomes a useful pivot point to see what other objects in our environment are interacting with this IP address or executing this command, giving us another lens to view regular or irregular activity. This gives us a whole new lens on our logs to determine what our objects are doing or what is happening on certain objects. So I could investigate the system acme-host as the risk_object or take a look at its threat_objects: the strange IP address 123.123.123.123, the command-line powershell.exe ExecuteMaybeBadThing, and the filename ReallySensitiveInfo.xlsx from various risk rules.

I found this helpful when I tuned to see how many other systems or users performed some activity that bubbled up into an alert, or to see at a glance which risk objects and threat objects interacted whenever we identified red team activity. There are also creative ways to create alerts off of threat objects themselves, or build some dashboards that slice up your risk index by these objects as a sort of threat hunting queue.

So What Does This Do?

Those are the mechanics – and I hope you're already connecting the dots to devise what you can do with them – but what does all of this allow you to do? A few things:

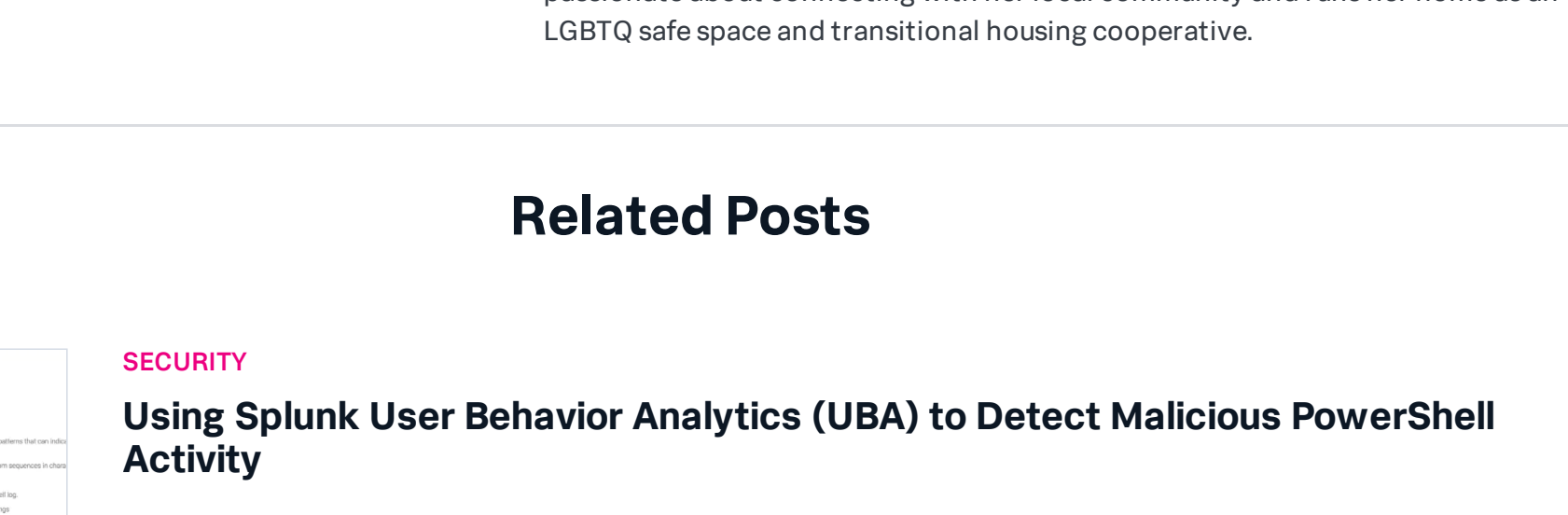
- Reduce the number of overall alerts while increasing the fidelity of alerts that arise
- Allow customers to define and produce internal threat intelligence to identify normal or anomalous behavior.
- Create high-value detections from traditionally noisy data sources, which align to popular cybersecurity frameworks like MITRE ATT&CK, CIS20, or the Lockheed Martin Cyber Kill Chain.
- Develop a valuable risk library of metadata-enriched objects and behaviors for manual analysis or machine learning.

And as I said before, this reduced workload and amplified ease between your security data, your detections, and your teams means more people can work together as their silos become increasingly interconnected and possibilities cascade outward.

But...?

This isn't a flick-the-switch solution; this is investing in your people with a product to transform your security approach. I am certain companies can adopt this approach with a number of other products (I have had friends who tell me they think they can figure it out), but we've got a bunch of awesome folks at Splunk who built a framework for you to get started and continuously work to make this happen as smoothly as possible. The transformations I see from folks who solve their security problems with the RBA methodology gives me hope for the next generation of security teams, who are hopefully less overworked and more empowered by the flexibility and capacity of the new standard for SIEM.


The way I see this journey progress is outlined below, and I will explain further in an upcoming blog.



How Do I Get Started?

That's a great question! Let's tackle this in the next blog, but you can check the last few years of [conf videos](#) to get more ideas. Keep up to date by subscribing to [Splunk Security Blogs](#) or [following me on Twitter!](#)



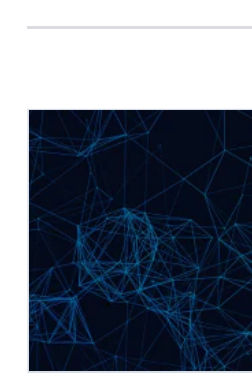
POSTED BY
Haylee Mills
 

Haylee Mills is a Security Strategist at Splunk, armed with the experience as a content detection engineer for a large financial technology company who transformed their security operations with risk-based alerting. Outside of work, Haylee teaches classes and mentors people looking to get into cybersecurity with a focus on BIPOC, women, and queer folks. She works as the Director of Development for local tech education organization Cybersecurity Council of Arizona, staff for the local cybersecurity conference CactusCon, and is part of the Tempe Arts & Culture Commission to advise the City Council on art development and preservation. She is passionate about connecting with her local community and runs her home as an LGBTQ safe space and transitional housing cooperative.

Related Posts



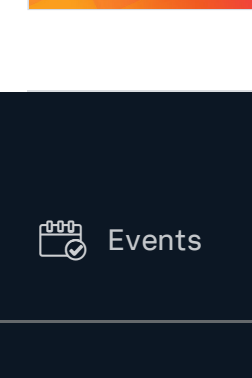
SECURITY
Using Splunk User Behavior Analytics (UBA) to Detect Malicious PowerShell Activity
By [Splunk](#) December 19, 2018



SECURITY
Hunting in a New Savanna
By [undefined](#) August 20, 2018



SECURITY
How Ernst & Young Helps Security Analysts Connect the Dots with Splunk SOAR
By [Splunk](#) September 04, 2020



SECURITY
Another Wireless Security Problem
By [Splunk](#) January 22, 2013

SPLUNK ON TWITTER
@Splunk
@Splunkanswers
@Splunkdev

SPLUNK ON FACEBOOK
Like us on Facebook
Like Splunk University on Facebook

SPLUNK ON LINKEDIN
Follow us on LinkedIn
Follow .conf on LinkedIn

SPLUNK SITES
Answers
Community
.conf

@SplunkUK
@SplunkDE
@SplunkGov
@SplunkforGood
@SplunkDocs

SPLUNK ON SLIDESHARE
Follow us on SlideShare

SPLUNK ON YOUTUBE
Subscribe to our Channel

Developers
Documentation
Splunk.com
Splunkbase

SPLUNK ON INSTAGRAM
Follow us on Instagram

Documentation
Splunk.com
Splunkbase
T-Shirt Store
Support
Training
User Groups