Turning Down the Noise
Get a Grip on Alert Fatigue

+1 (727) 914-5032 WWW.SP6.IO Service@SP6.IO

Systems made Secure. Compliant. Performant.

Over 50% Are False Positives

Over 40% of organizational Security Operations Centers (SOCs) experience more than 10,000 alerts each day. Of those, over 50% are false positives.

As a result, noise and alert fatigue often prove vexing to corporate IT departments.

Alert fatigue, which is also called alarm fatigue, occurs when analysts are overwhelmed by the sheer volume of system alarms going off - and become desensitized to them.

UNDERSTANDING THE PROBLEM

In under-staffed organizations, overworked analysts may be slow to detect and respond to data threats. Or they might ignore alarms altogether. In some cases, analysts suffer from job burnout and quit. Then, when new analysts are hired, the cycle repeats itself.

With the rise in security incidents, it’s important to be alert and on-point. Members of the SP6 services team have identified steps you can take that will help members of your team perform more effectively and improve your security coverage.

In today’s world of security monitoring, much emphasis is placed on alert tuning. But in trying to tune out as much noise as possible, you may exclude truly bad things from your result set. This is where Risk-Based Alerting (RBA) comes in.

WHAT'S RISK-BASED ALERTING?

Simply put, RBA is a system that increases the accuracy of alerts and provides an easily accessible alert narrative. It creates a framework allowing you to identify actions that raise the risk profile of people or assets.

SP6 uses RBA to make sure our monitoring teams are focusing on the right alerts while reducing the risk of tuning out threats.

Not only will RBA cut down on noise, but true positive rates will also significantly increase, as the riskiest events bubble up to the top.

ADVANTAGES OF RBA - SECURITY

The following security scenario takes place in Splunk Enterprise Security, where RBA allows technology teams to capably manage alerts. Splunk analysts create entity attributions and send them to the Risk Index in Enterprise Security. You are not directly generating alerts but forwarding them to the Risk Index. (You can also use behavioral patterns to set thresholds.)

As you create attributions, apply the appropriate context to them. Here is an example:

- Annotate an attribution with a relevant MITRE ATT&CK tactic or Kill Chain stage.
- Or apply a custom annotation of your choice.
- This turns the Risk Index into a collection of risky behavior you can mine.

It is important to note that each observation you send to the Risk Index may not indicate a threat on its own. However, it can indicate a threat when put in the context of risky attributions/annotations.

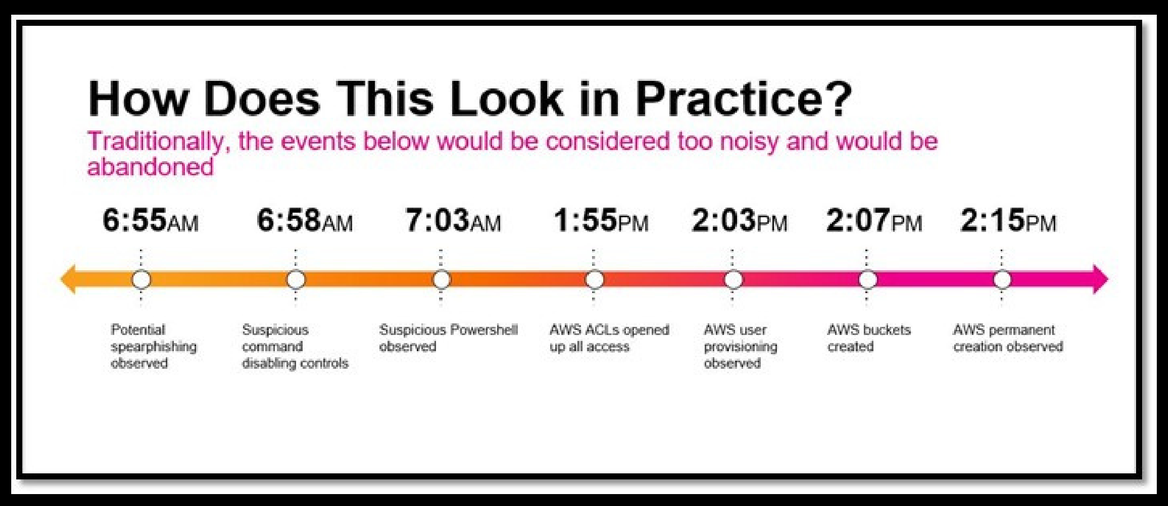
USING A RISK SCORE METHODOLOGY

An analyst can generate an alert when a user or system within your environment surpasses 100 within 24 hours. Or you can create a rule that says something like, “Generate an alert for each risk object with activity spanning three or more Mitre ATT&CK tactics over the past 14 days.”

By using this approach, you embed the value of cybersecurity frameworks in your detections and take them from concept to operational reality.

Another option is to scan for outliers in particular business units or active directory roles and generate alerts when a user’s risk score is one or two standard deviations above the normal for that unit or role.

Traditional Alerts



With Risk-Based Alerting

As depicted in the two graphics, the SOC created a rule where an alert is triggered any time a user exceeds an aggregated risk score over 100 in a 24-hour period.

By clicking into the alert, the analyst can see each attribution contributing to that alert in a Risk Message, giving them instant context. They will see that several lower-level alerts they could have overlooked or suppressed were all attributable to the same user and could pose a threat.

BENEFITS OF RBA - SECURITY

Reduce 60% - 80% of Alert Volumes

Once you initiate an RBA process within Splunk, your SOC team should notice a significant reduction in alert volumes – 60% to 80% in many cases. Some customers have lowered their abandoned percentage to nearly zero.

What's more, detection quality goes up. One customer reported their true positive rate doubled in the space of a few months. Others say they've been able to detect scenarios such as slow, prolonged attacks they would have had trouble detecting using traditional correlation searches.

Still, another benefit is that RBA will help you improve your security maturity and pinpoint areas you can improve upon. It's possible by taking the MITRE ATT&CK matrix, NIST, CIS 20, or any framework you choose. Annotate your searches with the relevant tactics, controls, or other framework components.

Finally, customers initiating RBA report a reduction in operational expenses.

How? You add more data sources and detections to your analytics. This, in turn, generates more alerts - and spurs the hiring of more analysts to review them. Only now, the analysts are working more efficiently.

Wouldn't you prefer that your SOC team focus on genuine security issues? They certainly would!

ADVANTAGES OF EPISODES - IT SERVICE INTELLIGENCE

Our next example of how to control noise and get a grip on alert fatigue also comes from Splunk, on the ITSI and observability side. Here, thresholds must be tuned properly. However, service owners aren't always sure when to alert.

Within ITSI, the Notable Event Aggregation Policy, or NEAP, helps to reduce noise. NEAP uses a correlation search to decide if it should sound an alert in each situation and group alerts into logical Episodes. Splunk correlation searches can be customized and enhanced.

It's a solution that can be built to scale, is highly performant, and is maintainable.

This is the Five-Step Process:

Step 1: Create Initial Notables.

Step 2: Group-Related Notables.

Step 3: Create Additional Notables.

Step 4: Add Alerting.

Step 5: Throttle Alerts.

BENEFITS OF EPISODES - IT INTELLIGENCE

As in the first example, an understaffed IT department plays a key role in perpetuating alert fatigue.

Let's say your company has seven web servers and they all crash at once. In most monitoring environments, alerts will pop up for all seven, but you won’t know if they’re related.

With ITSI and NEAP, these can be grouped into one episode or alert. (An SP6 Splunk expert could set that up for you.) The correlation search would run every minute, looking for whichever criteria you set up. It works on a scale of 1 to 6, with 1 being information and 6 is critical. And it can be configured to prevent over 100 different alerts.

We remember an SP6 client for whom we were sending alerts via a cloud-based IT service management (ITSM) software platform for the same problem because suppression wasn’t properly established. One of our engineers went in and focused the search.

(Note: Unlike Security, ITSI doesn’t deal with a lot of false positives. If the Key Performance Indicators are written correctly, they drive correlation searches.)

TAKE CONTROL OF YOUR NOISE AND ALERT FATIGUE

You've no doubt noticed that high-volume environmental noise can wear down even the most seasoned security team. This, in turn, makes your organization vulnerable to damage from actual threats-- but now you know some ways for those dual issues under control!

If you're having trouble getting noise from your security system under control, we recommend contacting an experienced company like SP6 which specializes in both high-volume environmental conditions and tuning alerts.

Your first step should be to partner with a company experienced in tackling these issues. SP6 has the knowledge and experience to identify any problems you may have.

Start by contacting us today for a no-cost, no-obligation consultation.