Sep 27, 2017 | Justin Bajko

Mistakes to avoid when measuring SOC performance

“What gets measured gets managed.” I heard this line repeated like a mantra early in my career whenever a new metrics program was being introduced in our security operations center (SOC). Unfortunately, nobody handed out magnifying glasses. That would have been helpful to read the six-point font metric-filled spreadsheet once it was printed out. We measured everything every manager could think to measure. The result? Our metrics improved but our outcomes didn’t.

For example, instead of taking the time to troubleshoot device outages when an associated ticket hadn’t been updated in a week, employees started simply updating the tickets with lines that said, “Device still not connected,” and moving on because they were being measured on the number of tickets worked. And this is the problem when you’re developing your first set of operational metrics. If you’re not thoughtful about the things that you measure and why you’re measuring them, you can end up managing to the wrong outcomes.

So, why do companies get it wrong so frequently? It’s not that they’re measuring the wrong things. Most often, companies are measuring the “right thing,” but they’re doing it in the wrong way or for the wrong reasons.

Here are the three most common mistakes I see companies make when they start measuring their SOC’s performance.

1. Counting all the things

Let’s start with these statements. Which do you think is better?

> We detected three more incidents this month! Success!

vs.

> We had three fewer incidents this month! Success!

How do you know what the right number is? More important, do you know *why* you’re counting these things in the first place? Are you concerned that you're missing things? If so, it probably makes sense to focus on uncovering more incidents. If you're focused on making your organization more resilient to attacks and you've spent a lot of effort on prevention, then it's reasonable to want to see a reduction in the total number of incidents. Either way, it's important to realize that the outcome you're trying to achieve can change, so using a metric like this by itself and without context is rife with risk.

Another popular metric is the aggregate number of alerts in "Low," "Medium," "High," and "Critical" severity buckets. Let's face it, "Critical" is what gets all the airtime. But watch out for misaligned objectives when it comes to severity. It's easy to perceive more value as you find more "super bad" things But it's easy for people to game the system when you look at things through this lens. Non-severe alerts start to get artificially dispositioned as critical and it can distract your team from real problems.

Finally, counting things for the sake of counting things can be bad for your team. People don't like being measured for reasons they don't understand or on things they perceive to be wrong. And believe me, they'll know it's wrong well before you do. If your team feels like they're spending their time on the wrong things or being evaluated in the wrong way, they'll leave.

2. Faster is always better

Speed is important when it comes to detecting and responding to threats. After all, if you're too slow, one compromised laptop can quickly spiral into an event where your most valuable data walks out the front door. But measuring people and processes based on speed alone can result in the wrong behavior. It can lead to quality issues -- and yet again -- drive people to game the system. Requiring your analysts to complete an investigation in 10 minutes sounds fine on the surface, but if you constrain an analyst's ability to actually dig into an incident and find out what's really going on for the sake of time, you're likely to miss critical details and negatively impact your response to that incident.

3. More money, more tools! (or is it less money, fewer tools?)

Everyone has a budget. And everyone gets measured on how they spend against that budget. That's not going to change any time soon, and I'm not advocating for it to change. However, spending less doesn't necessarily mean you're being a savvy spender. Likewise, spending more doesn't automatically make you more mature.

Cutting costs in the wrong areas can create visibility issues, make you more vulnerable, and ultimately create a level of risk that's far greater than the business truly understands. To complicate matters, if your cost cutting decreases your visibility, that'll make it even harder to calculate risk for the business.

But the flip side isn't exactly the promised land, either. Collecting all the latest cutting-edge security hotness that you heard about at RSA often does more harm than good. When you buy a new security tool, you need to have a plan for how you're going to use it: you need to understand what problem you have that this tool is supposed to solve, your team needs to know how to use it, and you guessed it, you need to know how you're going to measure its performance. What's the impact of throwing money at cool new technology without understanding how it fits into your organization? Oddly enough, it's similar to what happens when you try to cut costs without a plan - reduced visibility, increased vulnerability, and potentially increased risk to your environment.

And don't forget: how budgets get spent and what products to buy next are decisions that are often heavily influenced by what you're measuring. If you're measuring the wrong things, you allocate resources incorrectly and the vicious cycle continues.

So, what now?

Okay. I've spent a good bit of time talking about some of the most common mistakes that I see when organizations start to measure the performance of their SOC. Hopefully, I've whet your appetite to hear about some of the innovative things I've seen organizations do to effectively measure their SOC's performance. Stay tuned for our next post on this subject.

--

Visit the EXE blog for more articles like this at https://expel.io/blog