Sep 7, 2017 | Yanek Korff

Get your security tools in order: seven tactics you should know

At the tail end of the last century (doesn't that sound a lot longer ago than 17 years?), the Gallup organization surveyed 80,000 managers over the course of 25 years. Their goal was to understand what truly exceptional managers do differently to drive performance... and to create great places to work. Many of you are probably familiar with the book summarizing the results by Marcus Buckingham and Curt Coffman called "First, Break All The Rules."

I'll spare you the entire book summary and draw your attention to one particular bit. Their research pointed to twelve questions, which, when answered affirmatively, correlate to a high-performance work environment. And one of those questions (in fact it was #2 on the list) was the following:

> Do I have the equipment and material I need to do my work right?

Well now, that seems pretty straightforward. Of course you'd want your people to have the right tools for the job. Who wouldn't do that? Turns out, almost everyone.

Security operations centers (SOCs) are rife with inadequate, poorly integrated, dated technology that seems to frustrate security practitioners even if it's functional most of the time. Is there a SIEM sitting around whose care and feeding stopped a few years ago and seems to deliver little but false positives anymore? Did you pick an endpoint detection and response (EDR) solution that truly was "the new hotness" three years ago only now to discover that there's another "new new hotness" in town? Or my current favorite: state of the art network packet capture devices monitoring links that have no visibility into sensitive data moving between third-party cloud providers.

If you've hired well, these problems give rise to something interesting: intrepid security analysts spinning Python to work around limitations of existing technology and streamlining what they can. Does this help? Amazingly, it sure does. Being close to the problems and the associated technology means your analysts have unique insight into how to make their lives better. Go figure. The drawback? They're not software engineers. The solutions are brittle and difficult to maintain across churn.

Are we at an impasse then? Are we destined to be working with sub-optimal technology that does little more than confound us and get in our way? Well, yes and no. Here are seven things to keep in mind to bring harmony to your toolchain.

1. There are no perfect tools

Regardless of what you end up buying to solve your [insert security capability here] gap, the tool you choose will fall short in some way. Optimize for the capabilities that are most important to you and fill the gap another way.

2. Your imperfect tools need care and feeding

Negligence degrades your tools' performance. Maintaining operational rigor around maintenance is important, as is throwing out old tools when they've passed their prime.

3. Track capabilities

Whether you're talking about detection capability on the network, investigation capability on the endpoint, or vice-versa, keep an inventory of what tools are allegedly solving which problems. Avoid buying new tools just because it's fun.

4. Evaluate visibility

Beyond the capabilities your tools provide, each has a certain scope. Your EDR solution's visibility is governed by where agents are installed. Your packet sniffers can only see the links they're plugged into. Your security analysts are already in an unfair fight: make sure they're not fighting with blinders on.

5. Measure efficacy

You have assumptions when you buy new security products. Do your detectors detect with a good signal-to-noise ratio? Are your investigative tools used frequently? Track not only frequency of use, but how you're getting faster over time.

6. Integrate

Using imperfect tools is bad enough, hopping between frustrating consoles is worse. Encourage your security analysts to build software (ok, ok, write code) to mitigate alt-tab-copy-paste-death. To really turn it up to 11, invest in professional SOC plumbers (experienced software engineers) who understand the operational realities.

7. "Equipment and material" is more than tools

While we've focused heavily on tool choice in this post, operationalizing your tools is actually more important than their selection. Part of that is documentation. Playbooks. Without these, getting value out of your security investments depends on tribal knowledge, which is easily lost.

There are always clever new variations on old themes when it comes to security risks. Heck, some variations aren't even that clever or that new... but manage to ruin your day anyway. So, your security apparatus can't be

static either. Looking for a place to start? Once you get to the “acceptance” phase for #1 above, evaluate how well your existing tools are being maintained and address those gaps first. Work down the list from there.

As you press forward with this journey, realize that change will be constant. Optimizing for this along the way will help ensure your security toolset adapts to your changing needs. Your security analysts will thank you for it.

--

This is the first part of a five part series on key areas of focus to improve security team retention. Read the introduction, 5 ways to keep your security nerds happy*, or continue to* part two*.*