Adding a Twist to the Epic of Vulnerability Management

By Sam Curry, VP & CISO in Residence at Zscaler

Originally featured in CXO REvolutionaries online magazine

We are in our fourth decade since the Security Administrator Tool for Analyzing Networks (SATAN) hit the scene and we have to ask ourselves, "Why is it still so hard to effectively patch systems?"

> "History doesn't repeat itself, but it often rhymes."
>
> – Mark Twain

To be fair, the landscape hasn't exactly stayed the same: the adversaries, defensive tools, even the way we define vulnerabilities and how cybercriminals exploit them have shifted. Nevertheless, history does seem to rhyme an awful lot as we continue to struggle to collectively enhance our cyber defenses.

Let's dive into why—and how we can keep this perennial problem from rhyming into its fifth decade.

An expanding view of vulnerabilities

We can start by looking at vulnerabilities themselves and where they originate. The IT footprint has expanded to include entirely new types of infrastructure since SATAN hit the scene in April 1995: new development environments, programming languages, virtualization technology, API maturation, web services, shared responsibility clouds, and even entirely new computing paradigms.

The notion of a vulnerability itself has expanded to include misconfigurations, flaws in application development, process failures, risky user behavior, system weaknesses, business logic gaps, and more than we could have imagined during those first days of scanning the network. In response, we've seen a plethora of first-generation vulnerability scanners and aggregators across these domains, from countless companies, spanning free tools to the most expensive of kit. They all collect their findings but, of course, they don't agree on what they found, how to store the information, how to present it, or how to prioritize the discovered risks.

There is, it seems, always yet another vulnerability scanner (YAVS) in the conversation. Just when you think you've standardized, another rogue tool finds things other tools can't, an acquisition adds to the security stack, or a contractor introduces a new favorite. The response has been a fizzled revolution, not once but twice, in how to pull these tools together into summaries and reports and triage lists that, despite thousands of hours of work and the most amazing of Excel pivot table skills, continue to leave us with gaping windows of exploitability in most IT infrastructures.

All the while, attackers haven't sat idle. No matter how a vulnerability emerges, bad actors are ready to pounce faster than we can address issues. To make matters worse, they operate in closed labs that are well-funded and don't follow the nice rules of the vulnerability disclosure game. They prefer hoarding weaknesses and amassing arsenals for future "optionality," trickling them out into the wild for allies or the highest bidders.

The rate at which vulnerabilities are discovered continues to rise, even if only a fraction are ever exploited. A recent article in The Atlantic makes it even more clear from AI lessons in gaming that the situation is about to take a turn for the worse. IT explains how DeepMind produced opening moves and entire games for which Go grandmasters have no "Joseki" (an expected set of responses to openings and moves), leaving them feeling that they were watching an utterly alien game. We should expect new avenues and vectors for weakness and

exploitation in the much more fruitful field of exploitation to soon open up as the adversaries' labs go into full production leveraging the latest in technical innovation.

Challenges remain for defenders. IT departments should expect rapidly released patches will fail, as opposed to the lower chance of an exploit finding them with a particular roll of the device. The former's damage is less than the latter, but this sort of gamble is not one a manager should have to make, especially when history doesn't treat those who roll snake eyes kindly. Monday morning quarterbacking isn't just savage—it's potentially career ending.

And the revolutions in vulnerability and patch management? They just made the situation worse. Now there is always a record somewhere that disagrees on the right course of action. As automation starts to burn down the backlog, the scanners and aggregators keep making the task list stretch into the millions, increasing the certainty of self-inflicted interruptions by even the best meaning IT and security staff. Interestingly enough, patching isn't even the best answer (at least not every time). But how do you articulate that without a consistent perspective of the vulnerability landscape and topography?

The answer is to stop doing security incrementally with our heads down. As the novelist Rita Mae Brown wrote, "Insanity is doing the same thing over and over again and expecting different results." (No, it wasn't Einstein after all.) It's a wonderful opportunity for innovation and breaking out of the rhyming couplets of history we've been enduring over the last several decades:

- **We need a master system of record that is a *data* solution first.** This isn't a security problem. It's a data problem. Data solutions have addressed other problems and must be applied here. These must be flexible enough to look at our security gaps from a variety of vantage points—now a CVE, now a problematic user, now a vulnerable app. Such breadth and flexibility demands a cross-disciplinary approach. For that matter, we will also need to employ AI and good-old ML (since that seems to be forgotten as a critical tool in recent times) and to learn from large scale systems to support modeling, impact analysis, and so on all with respect to an accurate object model that has been de-duped, normalized, made referenceable, and generally cleansed from a data perspective. Do this right and we not only have tools monitoring real attacks but also the ideal way to simulate and game-out millions of attacks from which to learn and improve.
- **We need to factor in business context for risk prioritization, while also understanding the technical side.** This is counter-intuitive, but it's related to the point that patching isn't always the answer; and that's important when faced with that awful choice of a new patch versus a 10.0 critical vulnerability. It means we need to understand available avenues of attack and potential mitigating controls. We need to deploy faster on critical paths, especially where business impact is minimized. This is a multi-variable problem that needs business context and the topography of communications both, and right now it's more of an art being highly manual and dependent on luck and excellent Excel skills and a few people with deep tribal knowledge in any given IT environment. We need to turn these processes into a science.
- **Zero trust in the grandest sense is about reducing access by default—and its associated trust.** This means we must treat the internet as a Dark Forest (a wonderful answer from the world of Fermi's Paradox with lessons for us in IT and cybersecurity). To continue the Go analogy, this would be the equivalent of changing the board to deny intersection and moves for the adversary to attack: in the 19×19 grid of Go, there are 361 intersections to launch an attack. You might not be able to reduce those 361 avenues for offense in the board game, but we don't have to play by the rules in IT. We can change them with zero trust principles.

- **We should still demand that vendors work together, improve the quality of patches, and so on.** No one gets off free of responsibility here for making good code and ensuring its serviceability. Of course, there are no guarantees and it's a hard problem. So what – get to it.
- **There are still new standards needed and new things we can instrument in an almost meteorological sense from the neutral space between aggressors and defenders.** This is critical since we need to ultimately reduce the risk from attacks against all, and there is still a cybersecurity poverty line that doesn't benefit from well-resourced security departments. Vendors and services have to go down market, but we also need organizations like NOAA that understand through intelligent sampling what is really happening among all the players here, as well as work together on new ways of collaborating in defense.

Does the perfect solution exist today? No. And it's not about any one solution, but how multiple parts of the IT stack work together. Any cybersecurity strategy should focus on identity, endpoint, cloud, and so on, of course. But evolving beyond our acceptance of solid "D" grades in vulnerability and patch management will ensure we transcend the four-decade story of closing backdoors, opening secret entrances, suffering the consequences of misconfigurations, and accepting weaknesses that seem to proliferate faster than our ability to deal with them.

Concretely, this means that cybersecurity and IT practices together should be looking to the data plane and data structures for true systems of record, for vendors that work together, for integration of technical and business contexts, for rapid innovation, and for breaking out of the rhyming couplets of history. No one should accept sitting passively on the verge of 50 years in this epic of containing weaknesses and wondering why we seem no better at avoiding the mistakes of history.

Let's give this story a surprise twist. Let's ruin it for the villains for once.

About the Author: Sam Curry is a 30-year veteran of the cybersecurity industry. He began his career in signals and cryptanalysis and was the first employee at Signal 9 Solutions, a small start-up that invented the personal firewall, executed the first commercial implementation of Blowfish, and devised early stealthy (symmetric key) VPN technology that was ultimately sold to McAfee.

Sam would go on to serve as Chief Security Architect there and as head of Product for McAfee.com before holding several positions at RSA including head of RSA labs at MIT, head of product, and CTO, as well as Distinguished Engineer for EMC. After seven years with RSA, Curry acted as SVP and CISO at Microstrategy, CSO & CTO for Arbor Networks before it became Netscout, and as CSO for Cyberreason.

Sam is a Forbes contributor, holds 17 active patents in cybersecurity and a master's degree in counterterrorism, and sits on two boards of directors. In addition, he teaches courses at Harvard (online), Wentworth Technology Institute, and Nichols College. He is also a Fellow at the National Security Institute at George Mason University.
