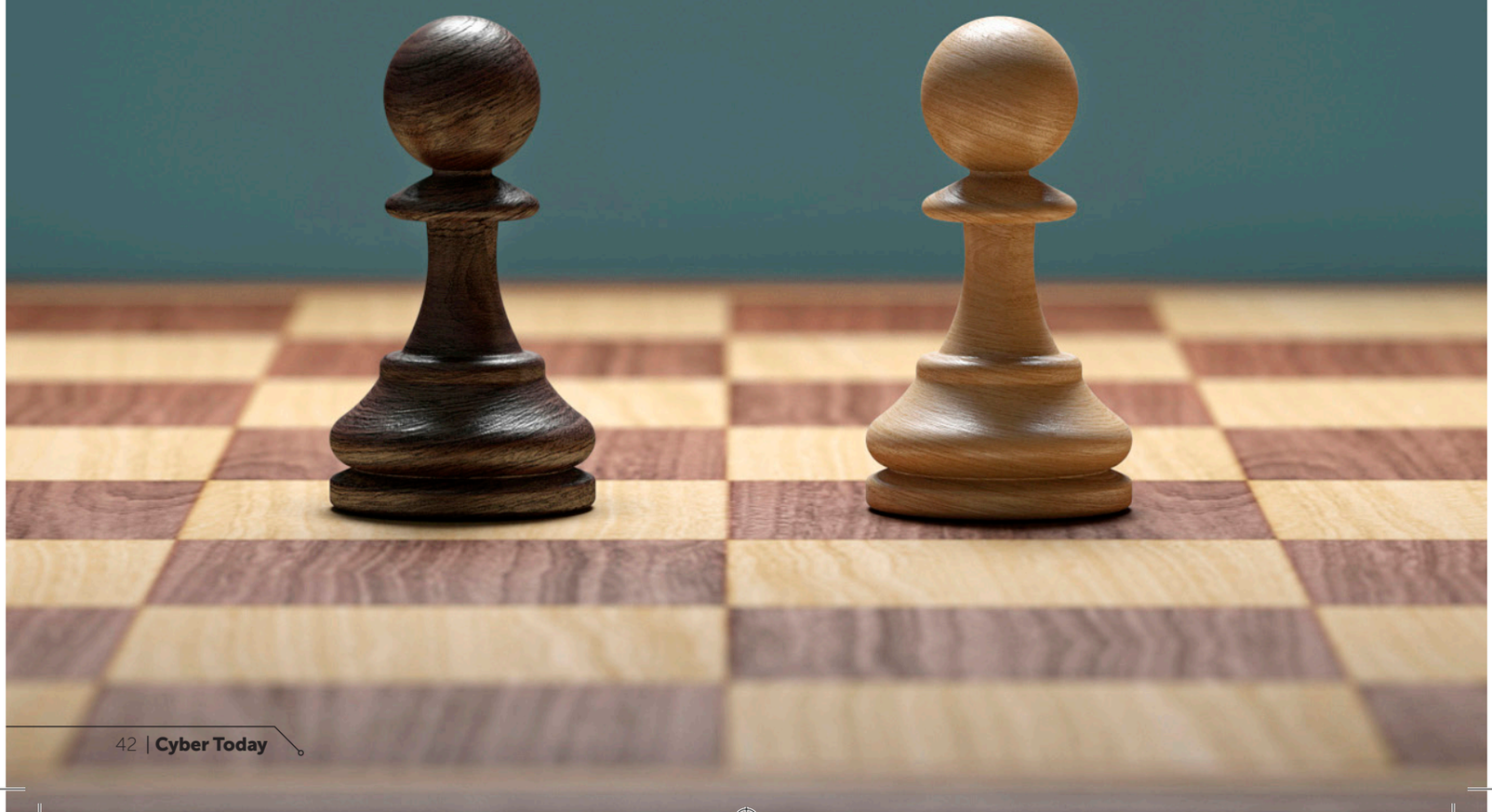
Who's winning in the game of attack and defend?

BY DR WADE BAKER, PROFESSOR, VIRGINIA TECH, AND PARTNER, CYENTIA INSTITUTE

It's often said that the 'playing field' of cyber security is heavily tilted in favour of attackers. Defenders must do everything perfectly, while attackers gain the upper hand if given the slightest opportunity. But is that an accurate depiction of the contest? Not exactly, according to recent research.



2580_Cyber Today Edition 2 2021.indd 42 9/7/21 2:52 pm

We recently had the opportunity to explore this attacker-defender dynamic through two massive datasets. Kenna Security provided vulnerability scan and remediation data on more than 13 million vulnerable assets by approximately 500 organisations that use their platform to prioritise vulnerability risk. Detections of attempts to exploit those vulnerabilities were contributed by Fortinet, which has security sensors deployed across tens of thousands of organisations.

Putting all that data together allowed us to produce Figure 1. The blue line shows the average time required by organisations to remediate vulnerabilities. Following that line shows that it takes about five months from when a patch is available for firms to remediate 80 per cent of vulnerabilities across their environment. The red shows the spread of exploitation attempts from the first organisation that detected related activity to the last (sometimes that's just a few firms; sometimes it's tens of thousands). Tracing that line reveals that it typically takes six months for attackers to reach 80 per cent of their target population.

The interplay between the attacker and defender timeliness tells a compelling story; attackers clearly have first-mover advantage (see the red shaded area from three months prior to patch until a week or so after), but defenders then kick it into high gear after patch release. They actually fix flaws faster than exploits spread in the wild for the next six months. After that, the law diminishing returns seems to set in and attackers steal back the momentum as defenders struggle with all those hard-to-find-and-fix assets strewn about their environment.

Figure 1 shows an overall average across all vulnerabilities affecting all types of assets; but the dynamics between attackers and defenders are much more varied than the clean set of curves depicts. Imagine

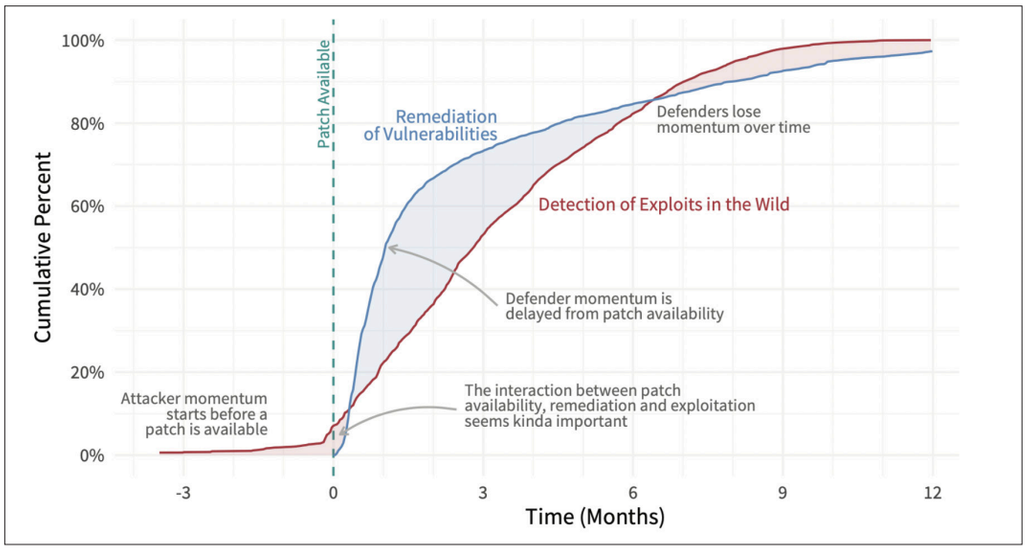


Figure 1

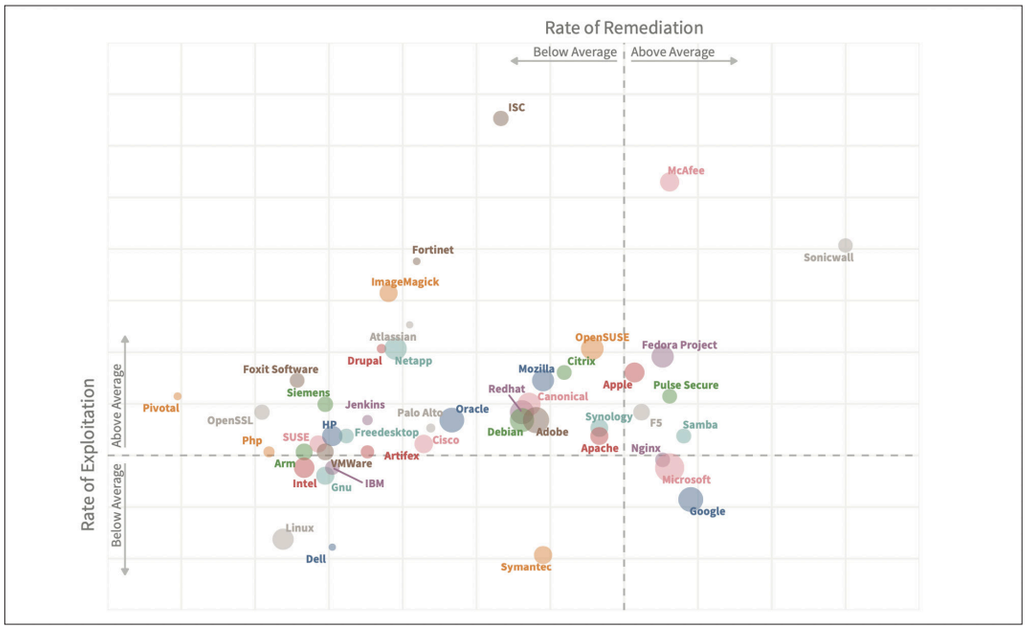


Figure 2

2580_Cyber Today Edition 2 2021.indd 43 9/7/21 2:52 pm

creating attacker-defender curves for each Common Platform Enumeration vendor, and then determining which ones are above and below average for remediation and exploitation. Sounds incredible, right? Well, that's exactly what Figure 2 depicts. Here's a quick summary:

- Vendors are plotted according to remediation (X-axis) and exploitation (Y-axis) rates.
- The dots for each vendor are sized relative to the number of detected vulnerabilities.
- The dashed lines separate overperformers and underperformers on each of those dimensions.

Based on these results, vendors have a heavy influence on both the rate of remediation and exploitation. Those in the lower-right quadrant, namely Google and Microsoft, are inherently more conducive to maintaining defender advantage. Despite their huge surface area of exposure, they're enabling defenders to remediate very quickly. This probably has a lot to do with their mature, coordinated disclosure programs and practice of frequent, automatic updates.

Vendors in other quadrants – especially in the upper-right – will make that feat more challenging. That's not to say your security destiny is determined solely by the software or hardware in your environment. But this strongly suggests that vulnerability management programs that adapt to the strengths and weaknesses of their tech stack are best positioned to reduce risk efficiently.

How does an organisation know if they're in such a position? Is it possible to determine the relative exploitability or remediability of an entire organisation? How does this factor into the probability of attacks and other risk measures? All of these are good questions worthy of exploration, but we're out of time and words for this article. Until we get more – may your blue curve remain well above the red. •

About the author

Dr Wade Baker *is a Professor at Virginia Tech and Partner at Cyentia Institute.*

2580_Cyber Today Edition 2 2021.indd 44 9/7/21 2:52 pm