What's the big deal about the new OWASP Top Ten?
(And what it means for your company's cybersecurity?)

During the next month, Founder & CTO John Matthew Holt will discuss the changes in the updated OWASP Top Ten list of web application risks. This week's focus is on the strategic shift represented by the list last updated in 2017. The following is an edited version of John Matthew's comments which you can listen to here.

Q: What's different in the 2021 OWASP Top Ten?

JMH: *The change between 2017 and 2021 is to move from an OWASP list that has been ordered roughly by incidents - what's the most frequent vulnerability type we see and let's put that at number one and what's the second most frequent vulnerability type we see and put it in number two, and so on - which was what we did in 2017, to a more strategic view.*

Instead, let's use data and collect data from the field - real world data - to drive a measurement that's based upon exploitability and impact. What we've seen by placing the emphasis on incidents is we can have developers and security professionals racing and chasing a very large number of vulnerabilities that in the scheme of things, may not matter simply because their incident rates is higher, but their severity and their impact might be low.

Q: What's has been the impact of focusing on incident rates instead of exploitability?

JMH: *Most applications today are naked. There's nothing inside that application stack that is actually looking at the application, looking at the code of the application, the memory, trying to identify when the application is kind of going off script, where it starts to behave in unintended and undesirable ways.*

In the past, we've relied on perimeter security like firewalls and things like this to create this idea of a moat around our applications and data, which is, you know, the things that are important to us as organizations. That barrier that that we trusted 10, 15 years ago is now very porous. And so, the frontline has moved.

Q: How will a more strategic OWASP Top Ten help improve cybersecurity?

JMH: *Waratek and the agents and autonomous security sensors that we build is a really important change in the way people can view the security posture of their applications. Suddenly their applications aren't naked anymore. It's got clothes. It's got armor, it's got defense.*

Listen to John Matthew's full comments on the shift in the 2021 OWASP Top Ten (Time to Listen - 3:33)

Next week: The most important items on the 2021 OWASP Top Ten