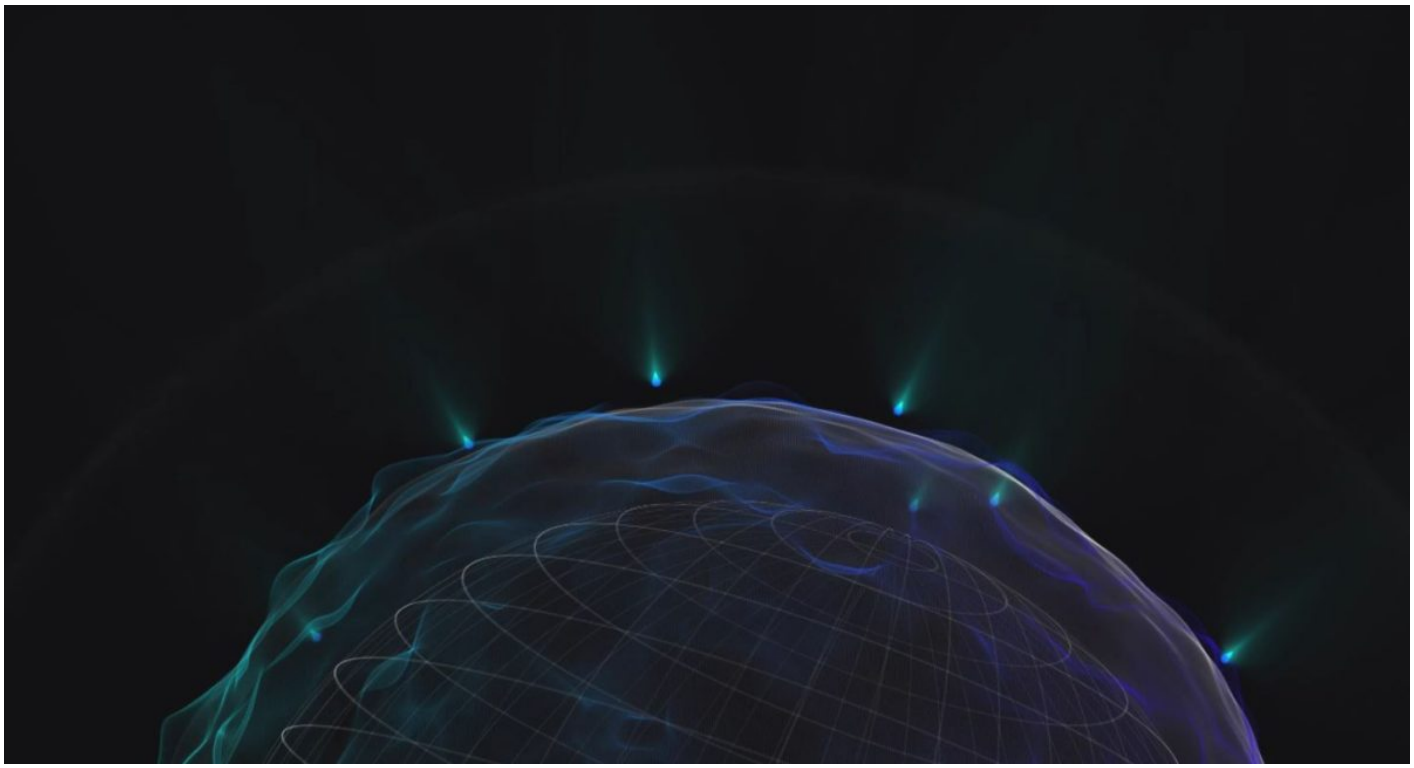
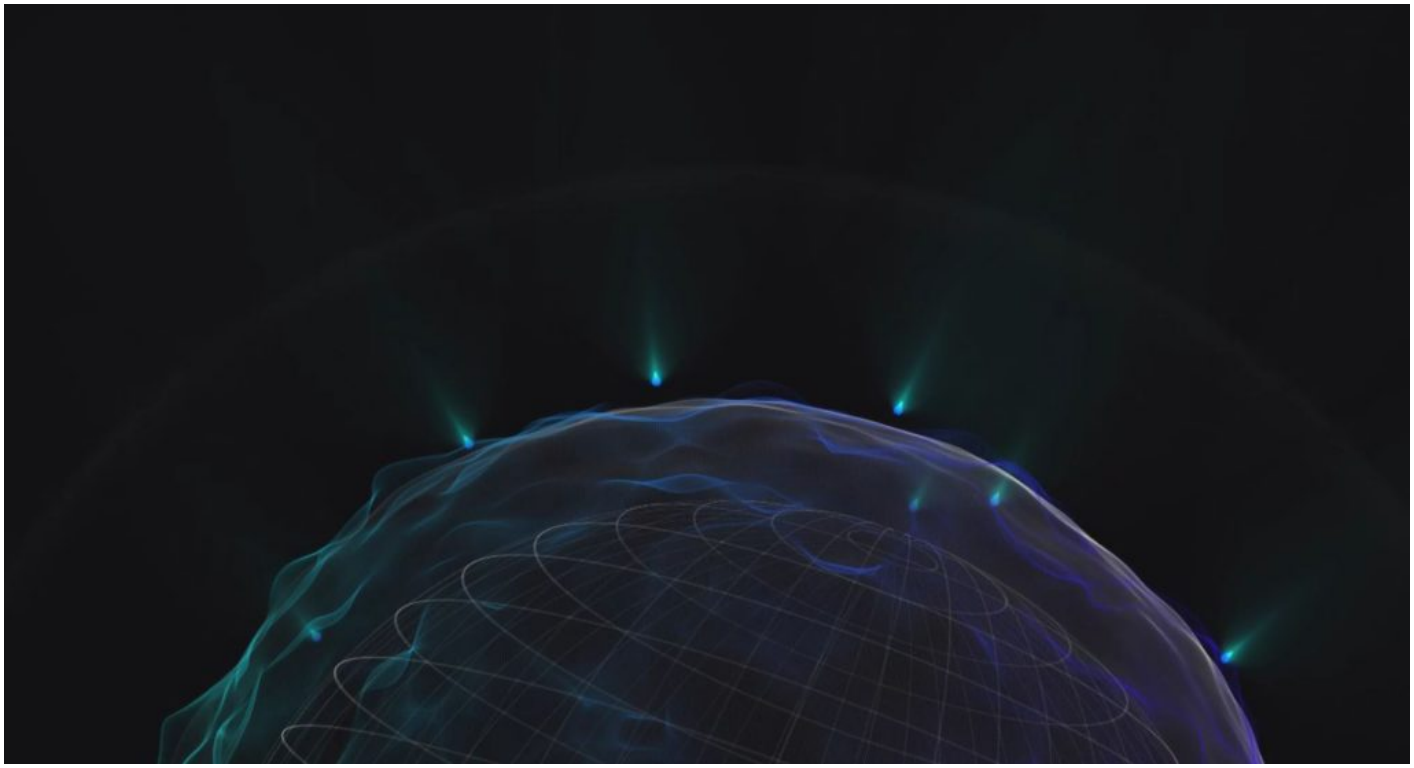
# Cyber Attack Simulation: the new test in town





When was the last time you had a penetration test of your network or a vulnerability assessment? Penetration testing has traditionally been an annual event for most organisations. Of late we have seen vulnerability assessments delivered as a service with the ability to run tests on demand. Invariably vulnerability assessments are still run once a year oftentimes due to resource shortage and in many instances it's just not a high priority because nothing bad has happened – or at least we are not aware of it.

On the other hand, industry security statistics would indicate that the general approach to security could well be a disaster waiting to happen, or worst still a disaster that has happened but just not discovered yet. Yes we know that enterprise organisations and some medium sized organisations have a highly security regime in place and manage security according to best practices. Despite the efforts of the aforementioned organisations the numbers are still overwhelmingly in favour of the bad guys as illustrated below.

- 100% of organisations interact with known malware sites – simply put, everyone is likely to be infected at some stage
- 99 days average time to detect a breach of a pool of known vulnerabilities
- 4 hours average time it takes cyber attackers to steal data
- 365 days – time between vulnerability assessments and penetration tests

For sure both vulnerability assessments and penetration test have proven to be valuable tools in the arsenal for protecting IT systems from compromise, but only when used effectively and frequently enough.

One challenge however that either approach may find very difficult to keep up with is the rate of change as newer, more sophisticated and persistent threats and exploits appear on an almost daily basis.

An emerging approach to confront the threats head on while enabling organisations to take the initiative is to deploy a solution that conducts a series of simulated attacks based on known and emerging threat vectors. With this type of approach, you can now address the question “how do you know your security systems are working?”.

How many times have you seen a detailed and impressive list of access control lists only to be undone by the second to last line “permit ip any any”.

Without comprehensive and persistent testing, any assurance of cyber security is based purely on assumption and best guess.

Yes you have defences in place such as firewalls, endpoint security, anti-malware solutions but how do you know that they are really effective against known/unknown cyber threats. The assumption is that you have the right defences in place to protect from vulnerabilities and they security solutions are optimally configured. You only truly know for certain when an attempted breach has been attempted, detected and blocked. On the other hand you may have been hacked and you either never know or you don’t know for months after the event when the hackers have stolen day and moved on to other victims.


A simulated attack is a method of safely checking whether your systems are safe and your data is protected from vulnerabilities. The simulation can run a range of attack vectors to test your defences against a range of vulnerabilities. Simulated attacks that are successful will give you a clear understanding of your current vulnerabilities and how to mitigate them – it gives

you actionable intelligence of the holes in your cyber defences. It can also validate the security controls that are in place and be used to test your security incident response procedures. Remember cyber defences is not just about preventing attacks, it’s also about what you do when the attacks occur to remediate and recover.

A simulated attack service can also be used to undertake real time validation especially when changes are made or as you become aware of new vulnerabilities. When run as a cloud service, it can be run repeatedly to provide ongoing security posture assurance. A simulated attack service is definitely a service worth considering augmenting a comprehensive security posture assessment approach that includes penetration testing and vulnerability assessment. Simulated attacks can be seen as an emerging solution that is geared to match the rapid and changing nature of cyber threats.