The NopSec Risk Score

The NopSec Risk Score improves vulnerability prioritization by leveraging the power of machine learning to combine likelihood of attack with environmental impact to give organization a true view of their risk posture.

CVSS vs NopSec Risk Score

CVSS (Common Vulnerability Scoring System) is the industry-standard way of assessing the severity of security vulnerabilities.

CVSS was designed to measure the technical severity of a vulnerability, but is widely misused as a means of vulnerability prioritization and assessing risk.

CVSS base score does not account for temporal evolution of a vulnerability (existence of exploits, malware, etc.) and user context (asset value) and as such does not reflect the real risk posed by a vulnerability.

It is neither efficient nor safe to prioritize vulnerabilities based on CVSS, as it marks too many vulnerabilities as high or critical while scoring many of the truly dangerous ones as medium or low severity.

See our 2018 State of Vulnerability report and the CERT/CC Towards Improving CVSS paper for more.

BETTER PRIORITIZATION

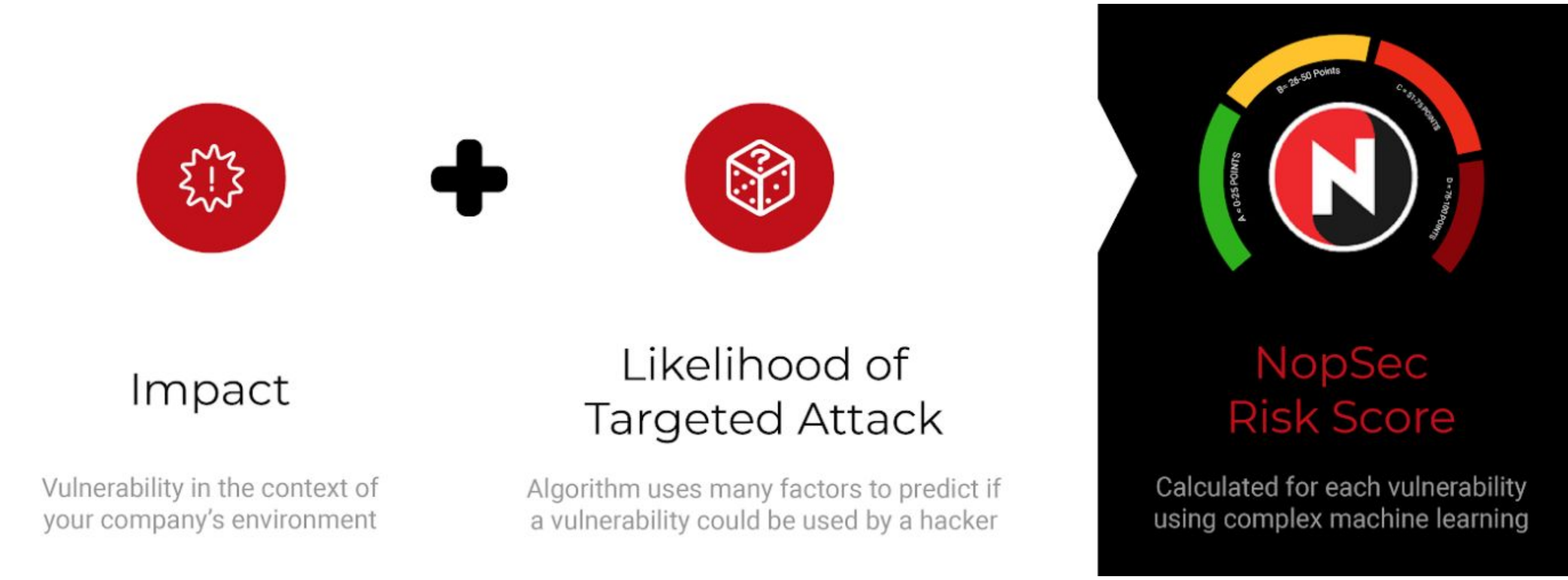
4x

CVEs with critical NopSec risk score are 4 × more likely to have threats associated with them than CVEs with critical CVSS.

2x

Critical NopSec risk score is 2 × better at predicting actual threats than critical CVSS score.

That is why NopSec has created Unified VRM - powered by automation and machine learning. The solution dramatically reduces the turnaround time between identification of critical vulnerabilities and remediation, helping organizations avoid attacks and costly data breaches.



Likelihood of Targeted Attack

Our technology gathers historical data about vulnerabilities and leverages up-to-date threat intelligence in our ML algorithms to find vulnerabilities most likely to be used in malware or targeted attacks.

NopSec vulnerability risk is derived based on hundreds of features incorporating: basic vulnerability information, vendor and product information, vulnerability descriptions, exploit information, and social media feeds.

Environmental Impact

Unified VRM ingests data about your environment to give context to each vulnerability.

Using that, we re-prioritize vulnerabilities found in your environment according to this risk and the criticality of the assets they were found on.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com