CYBREYE

CYBERSCORE

A clear measure that tells you how protected your organization is from Cyber Threats

CYBERSCORE BENEFITS

There are many benefits to having a cyber risk score, based on the current state of your IT environment as assessed against the full landscape vulnerabilities.

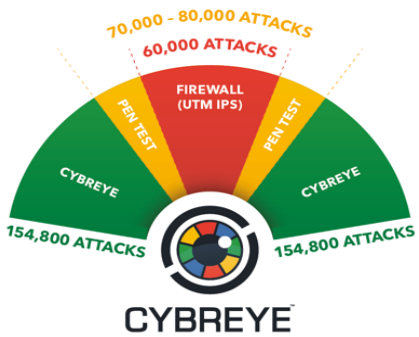
The score is derived as part of the Cybreye Security Assesment and your enviroment can be re-scored when vulnerabilities found have been remediated.

A Cybreye CyberScore can:

- Help your security team professionals address gaps, and the boards of those companies prioritize security investments.
- Enable third parties, from partners and potential customers to insurers, understand a firm's security risk.
- It can help you to perform cyber due diligence by gaining actionable intelligence on the security performance of a merger or acquisition target.

YOUR CYBERSCORE IN REALTIME

Cybreye's comprehensive Security Assessment tests against 154,000+ attack vectors per IP, which is over 65,000 more threats than the best available commercial assessment.



YOUR SCORECARD

Your CyberScore forms part of your overall ScoreCard for each IP or Domain which comprises a domain Total Score as well as the actual number of Critical, High Impact and Medium Impact vulnerabilities.

THE CYBREYE CYBERSCORE

CRITICAL SEVERITY: Score 9-10

Allows any user with minimum technical skill to compromise the affected system.

HIGH SEVERITY: Score 7-8

Permits a malicious user to directly interfere, at the administrative (i.e. root) level, with the structure and functions of the target system via a single vulnerability.

MEDIUM SEVERITY: Score 4-6

Permits a malicious user to externally tamper with the normal operations of a target.

The Cybreye CyberScore is based on the Michael Hayden (a retired United States Air Force four-star general and former Director of the National Security Agency and Director of the Central Intelligence Agency) scoring mechanism for vulnerabilities exposed by penetration testing.

Under the Cybreye CyberScore, any Critical vulnerabilities found during a Cybreye Security Assesment are scored as a 9-10. High Impact vulnerabilities are scored as a 7-8 and Medium Impact vulnerabilities as a 4-6. Vulnerabilities scoring 1-3 are generally informational and typically should not have a direct impact on the environment, so have been excluded from the Cybreye CyberScore.

This means that if an external facing IP's of an individual enterprise was assessed and they had 10 of the highest critical and 10 of the highest high impact vulnerabilities their CyberScore would be 180. Clearly the lower the CyberScore the better the resulting position of that IP asset. A perfect score would be zero.

Where an assessed Domain has multiple IP's the Cybreye CyberScore is the average of those IP's assessed.