HADRIAN

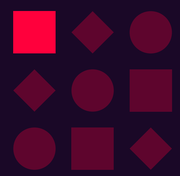
Dieci motivi per cui il monitoraggio continuo della superficie di attacco è fondamentale

Con l'espansione online delle organizzazioni, la costante supervisione della superficie di attacco - i punti vulnerabili all'accesso non autorizzato - diventa fondamentale per contrastare le minacce informatiche in continua evoluzione. L'identificazione e la gestione proattiva dei rischi permettono di proteggersi da tali minacce. Hadrian esegue scansioni continue della superficie di attacco, individuando tempestivamente i rischi per ridurre la probabilità di un attacco efficace.

Entro **15 minuti** dalla scoperta di una vulnerabilità, gli hacker iniziano a lavorare per sfruttarla.

10%

di tutte le vulnerabilità identificate (CVE) è classificato come critico.



Una vulnerabilità su dieci nelle applicazioni accessibili da Internet è considerata ad alto rischio o critica.

delle organizzazioni ha subito un attacco mirato a un asset rivolto a Internet sconosciuto, non gestito o gestito in modo inadeguato.

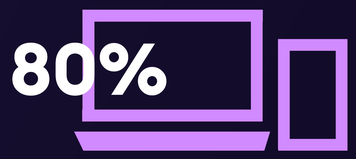
Le segnalazioni per configurazioni errate dei siti web sono aumentate del **151%** nell'ultimo anno.

L'**84%** delle aziende presenta vulnerabilità ad alto rischio sui propri perimetri di rete.

Le vulnerabilità non corrette sono state la causa del **60%** delle violazioni dei dati.

Si stima che le grandi organizzazioni che distribuiscono codice in produzione quotidianamente passeranno dal **5%** nel 2021 al **70%** nel 2025.

L'**80%** degli exploit pubblici viene reso disponibile prima della pubblicazione dei CVE.



dei CISO (Chief Information Security Officer) afferma che aggiornamenti critici o patch, sebbene appaiano correttamente distribuiti, non hanno in realtà interessato tutti i dispositivi.