Principales conclusions du rapport

Les API basées sur l'IA sont moins sécurisées que leurs homologues.

La majorité des API basées sur l'intelligence artificielle (IA) sont accessibles en externe et beaucoup dépendent de mécanismes d'authentification inadaptés, une faille aggravée par le nombre croissant d'attaques pilotées par l'IA qui visent ces API.

L'IA alimente les avancées techniques des acteurs malveillants.

Cela inclut des progrès tels que les logiciels malveillants pilotés par l'IA, l'analyse des vulnérabilités, les attaques sur les systèmes intégrant l'IA et les capacités sophistiquées d'extraction Web.

32 %

Pourcentage d'augmentation du nombre d'incidents liés aux 10 principaux risques pour la sécurité des API selon l'OWASP

Les risques pour la sécurité des API ne cessent de se multiplier. En effet, la liste des 10 principaux risques pour la sécurité des API dressée par l'Open Worldwide Application Security Project (OWASP) révèle des failles d'authentification et d'autorisation qui exposent les fonctionnalités et données sensibles.

30 %

Hausse des alertes de sécurité liées au cadre de sécurité MITRE

Les pirates utilisent des techniques sophistiquées, notamment l'automatisation et l'IA, pour exploiter les API. Le cadre de sécurité MITRE permet d'identifier plus rapidement et plus précisément ces attaques.

33 %

Pourcentage d'augmentation des attaques Web d'une année sur l'autre, à l'échelle mondiale

L'augmentation des attaques est directement liée à l'adoption rapide des services cloud, des microservices et des applications d'IA, qui élargissent les surfaces d'attaque et posent de nouveaux défis en matière de sécurité.

+ de 230 milliards

Nombre d'attaques Web qui ciblent les entreprises commerciales, ce qui en fait le secteur d'activité le plus touché, avec près de trois fois plus d'attaques que le secteur des hautes technologies (qui arrive en deuxième position).