I principali risultati emersi dal rapporto

Le API basate sull'AI sono meno sicure delle loro controparti.

La maggior parte delle API basate sull'intelligenza artificiale è accessibile dall'esterno e spesso si basa su meccanismi di autenticazione inadeguati, una vulnerabilità che diventa più pericolosa se si considera l'incremento degli attacchi basati sull'AI a cui sono soggette.

L'AI favorisce il progresso tecnologico dei criminali.

Le tecniche più innovative comprendono i malware basati sull'intelligenza artificiale, le soluzioni per la scansione delle vulnerabilità, la violazione dei sistemi che integrano l'AI e funzionalità avanzate di web scraping.

+32%

Aumento degli incidenti correlati alle 10 principali vulnerabilità della sicurezza delle API riportate nell'elenco OWASP.

Gli incidenti di sicurezza delle API sono in aumento e l'elenco OWASP mette in luce le falle dei sistemi di autenticazione e autorizzazione che rendono visibili le funzionalità e i dati sensibili.

+30%

Aumento degli avvisi di sicurezza correlati al framework MITRE.

I criminali sfruttano le API attraverso l'impiego di tecniche avanzate, come l'automazione e l'intelligenza artificiale. Il framework MITRE può aiutare gli addetti alla sicurezza a identificare questi attacchi con maggiore efficienza e velocità.

+33%

Aumento degli attacchi web globali su base annua.

La diffusione degli attacchi è direttamente correlata alla rapida adozione di servizi cloud, microservizi e applicazione AI, che ampliano le superfici di attacco e pongono nuovi rischi per la sicurezza.

Oltre 230 miliardi

Attacchi web che hanno colpito il commercio.

Questo settore è stato il più colpito e ha segnalato un numero di attacchi quasi tre volte superiore a quello dell'high-tech (situato al secondo posto).