Come l’AI ha già stravolto l’intero settore della cybersecurity



Ci sono momenti in cui i freddi dati numerici possono spazzare via le speculazioni di chi prevede un futuro completamente diverso da ciò che siamo abituati a considerare “normale”. Ci sono momenti in cui, però, quegli stessi dati numerici finiscono per **confermare le peggiori previsioni**. A guardare le cifre riportate dal 2026 Y-Report di Yarix e dalle dichiarazioni degli esperti della italianissima azienda di cyber security, l’ipotesi di un futuro dominato dall’AI è qualcosa di più di una semplice suggestione.

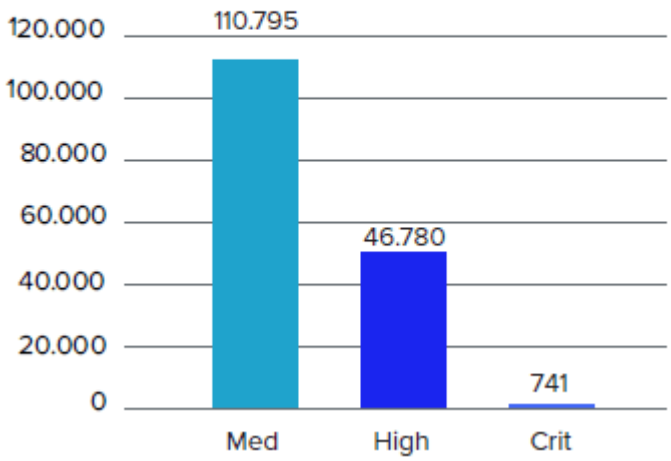
Un’ondata di attacchi

A fare impressione, nel quadro tratteggiato dal rapporto, sono prima di tutto i numeri. I dati raccolti riguardano infatti circa 240 aziende italiane, ma le segnalazioni di eventi di cyber sicurezza sono nell’ordine delle decine di migliaia. Più

precisamente, **nel corso del 2025 il Security Operation Center (Soc) di Yarix ha registrato ben 522.486 eventi**, cioè "possibili violazioni dei livelli di sicurezza definiti o situazioni anomale potenzialmente rilevanti per la protezione dei dati e degli asset aziendali".

Di questi, ben il 30% (158.316) sono stati classificati come veri e propri incidenti di sicurezza, cioè "uno o più eventi che determinano, o possono determinare, la compromissione della riservatezza, dell'integrità o della disponibilità dei dati e dei servizi informatici"**. In media, quindi, stiamo parlando di circa 658 incidenti di sicurezza per azienda. Quasi due al giorno**.

Fig. 2 - Eventi suddivisi per gravità



Un valore **in costante aumento**, che gli esperti di Yarix imputano alla costante evoluzione delle tecniche di attacco e, in particolare, all'utilizzo di strumenti basati sull'AI da parte dei criminali informatici che consentono di utilizzare modelli di attacco più distribuiti, automatizzati e adattivi.

Il fattore tempo

Uno degli aspetti più preoccupanti è il continuo assottigliamento delle tempistiche di attacco. Gli autori del report, infatti, segnalano una notevole riduzione del tempo tra accesso iniziale e potenziale impatto dell'attacco

informatico.

Si tratta di uno dei nodi fondamentali in ambito cyber security, soprattutto da quando il fenomeno dei ransomware ha assunto un ruolo di primo piano. **In chiave offensiva, l'uso dell'AI ha permesso ai cybercriminali di ridurre notevolmente i tempi necessari** per quella che in gergo viene chiamata *weaponization*, cioè l'attività di trasformare una vulnerabilità conosciuta in un exploit pronto all'uso.

Nell'ottica di chi si trova sul fronte difensivo, questo significa essere in grado di individuare nuove forme di attacco con una velocità maggiore rispetto al passato. La risposta, come prevedibile, è solo una: affidarsi all'AI. Le cose, però, non sono così semplici.

Il fattore volume

La rapidità con cui i criminali informatici sono in grado di sviluppare strumenti offensivi si traduce, nella pratica, in un numero impressionante di attacchi che rischiano di sommergere letteralmente i team di specialisti dedicati all'analisi delle minacce. A livello di Soc, il rischio è che la quantità di alert rilevati finisca per "intasare" i processi di analisi lasciando via libera alle attività dei cyber criminali.

L'AI, in questo ambito, viene attualmente utilizzata in affiancamento agli analisti per migliorare le prestazioni a livello di tempistiche, senza però sostituire completamente l'elemento umano. Secondo gli esperti di Yarix, però, il contesto porta a osare di più. "**A fine luglio eseguiremo il primo test operativo per gestire un Soc L1 interamente con l'intelligenza artificiale**" dichiara Mirko Gatto.

Il "livello 1" dei Security Operation Center è quello dedicato alla prima analisi degli eventi di sicurezza, a cui è affidato in sostanza il compito di scremare gli alert per eliminare i

falsi positivi e individuare gli eventi sui quali vale la pena approfondire l'analisi. Il ruolo "umano" resta comunque fondamentale per L2 (approfondimento) e L3 (intervento per il contenimento della minaccia).

Un notevole passo avanti, che lo stesso manager di Yarix annuncia con una certa cautela, ma che chiarisce meglio di qualsiasi altra considerazione la pressione a cui sono sottoposti gli addetti ai lavori in questa fase. **Il rischio di affidare completamente la fase di prima analisi degli eventi all'intelligenza artificiale, infatti, riguarda essenzialmente la possibilità che non riescano a valutarne correttamente la rilevanza**. Un rischio che, però, vale la pena di affrontare. "Il tema dell'alert fatigue è sempre stato un tema rilevante del Soc, quindi la capacità di ridurre i falsi positivi rilevati dall'AI sarà uno degli aspetti su cui il mondo della cyber security dovrà concentrarsi attraverso l'affinamento del prompting" sottolinea Gatto. "Personalmente sono ottimista" conclude.