HACKTHEBOX

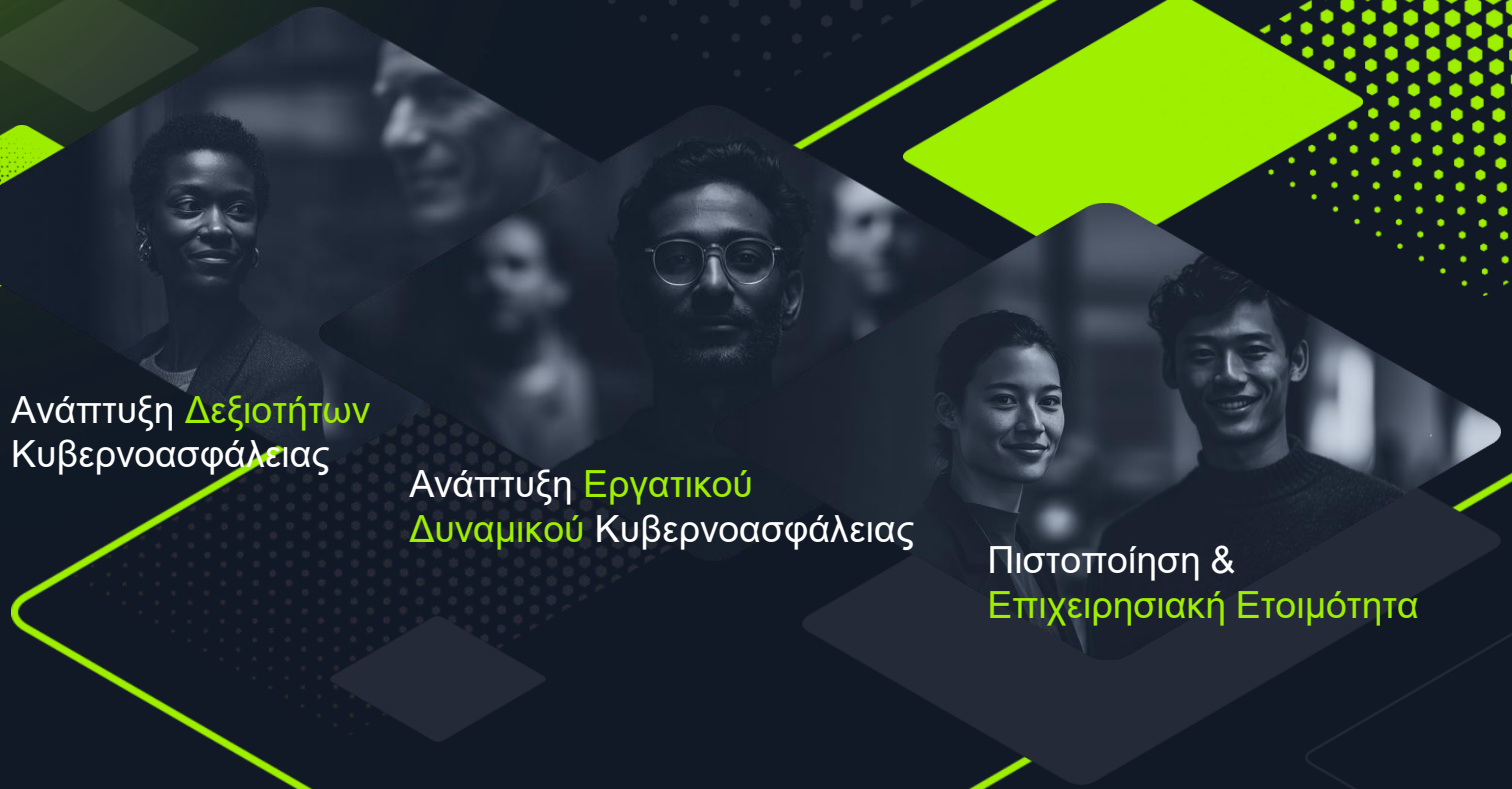
Hack The Box

Μια ολοκληρωμένη λύση cyber readiness και ανάπτυξης δεξιοτήτων cybersecurity ομάδων.

Οι κορυφαίες cybersecurity ομάδες
δεν δημιουργούνται στις αίθουσες διδασκαλίας.
Διαμορφώνονται μέσα από συνεχή ανάπτυξη δεξιοτήτων,
επικυρωμένη από τις απαιτήσεις του κλάδου.

Η **Hack The Box** μετατρέπει τη μάθηση σε βίωμα,
προσελκύοντας τα πιο προηγμένα ταλέντα στον χώρο,
βοηθώντας τους να αναβαθμίζουν συνεχώς
τις δεξιότητές τους σε κορυφαίο επίπεδο.

Τι Προσφέρουμε



Ανάπτυξη Δεξιοτήτων Κυβερνοασφάλειας

Ανάπτυξη Εργατικού Δυναμικού Κυβερνοασφάλειας

Πιστοποίηση & Επιχειρησιακή Ετοιμότητα

Εκτεταμένη Κάλυψη Cyber Domains & Ρόλων

Offensive

- (Web) Penetration Tester
- Red Team Operator
- Cloud Penetration Tester
- AI Red Teamer etc.

Defensive

- SOC/DFIR Analyst
- Malware Analyst
- Detection Engineer
- SIEM Engineer
- Cloud Security Engineer etc.

General IT & Mgmt

- Software Developer
- IT Manager
- NOC/SOC Manager
- GRC Analyst
- CISO / DPO

Cyber Mastery

2.200+
εργαστήρια και εκπαιδευτικό περιεχόμενο

Νέο εκπαιδευτικό υλικό **σε εβδομαδιαία βάση**

9 αναγνωρισμένα προγράμματα πιστοποίησης

1 αναγνωρισμένο certificate program από US DoD 8140

Community Inspired

4.3M+
μέλη στις πλατφόρμες

19M+
ώρες εξάσκησης / έτος

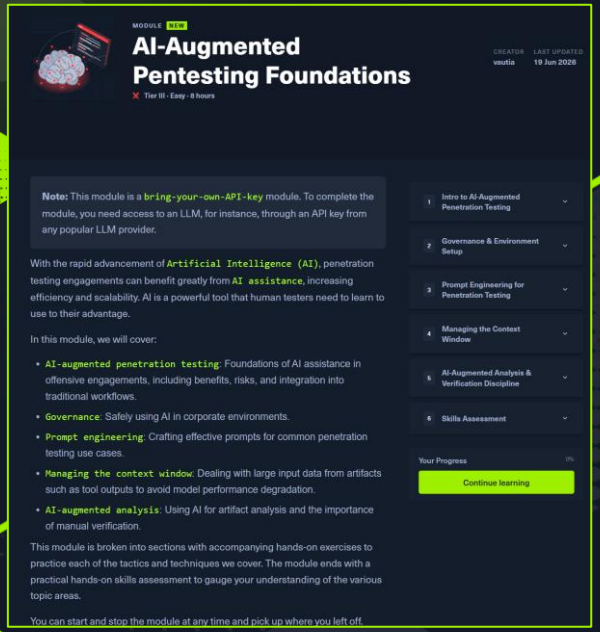
131 τοπικές κοινότητες και συναντήσεις

Enterprise Trusted

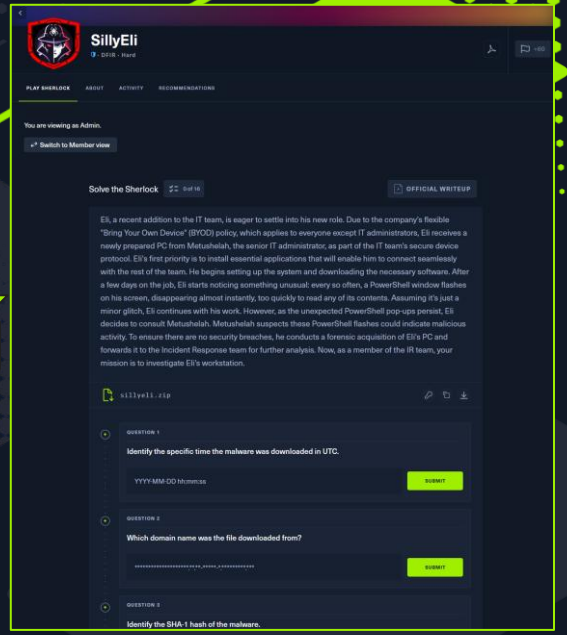
1.5K+
οργανισμοί, συμπεριλαμβανομένων εταιρειών Fortune 100

PUMA · EA SPORTS · TOYOTA · SIEMENS · Deloitte. · intel

Πως Το Προσφέρουμε

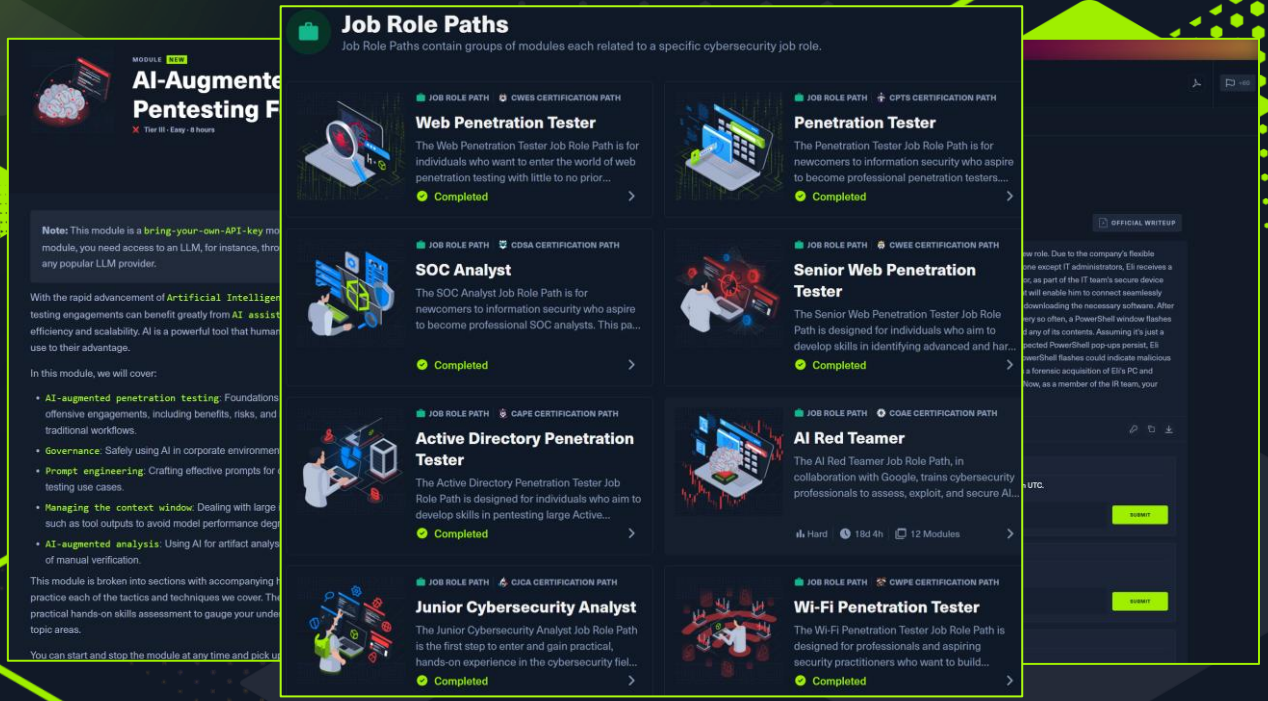


Θεωρία



Εξάσκηση

Πως Το Προσφέρουμε



Θεωρία

Πλάνα Εκπαίδευσης

Εξάσκηση

Πως Το Προσφέρουμε

Πιστοποίηση

Θεωρία

Πλάνα Εκπαίδευσης

Εξάσκηση

Μετρήστε την απόδοση και την αποτελεσματικότητα των ομάδων σας

Καθορισμός στόχων σε συνεργασία με εξειδικευμένους Customer Success Managers της HTB

Δοκιμάστε στην πράξη τα playbooks σας και επιβεβαιώστε τις γνώσεις που έχουν αποκτηθεί

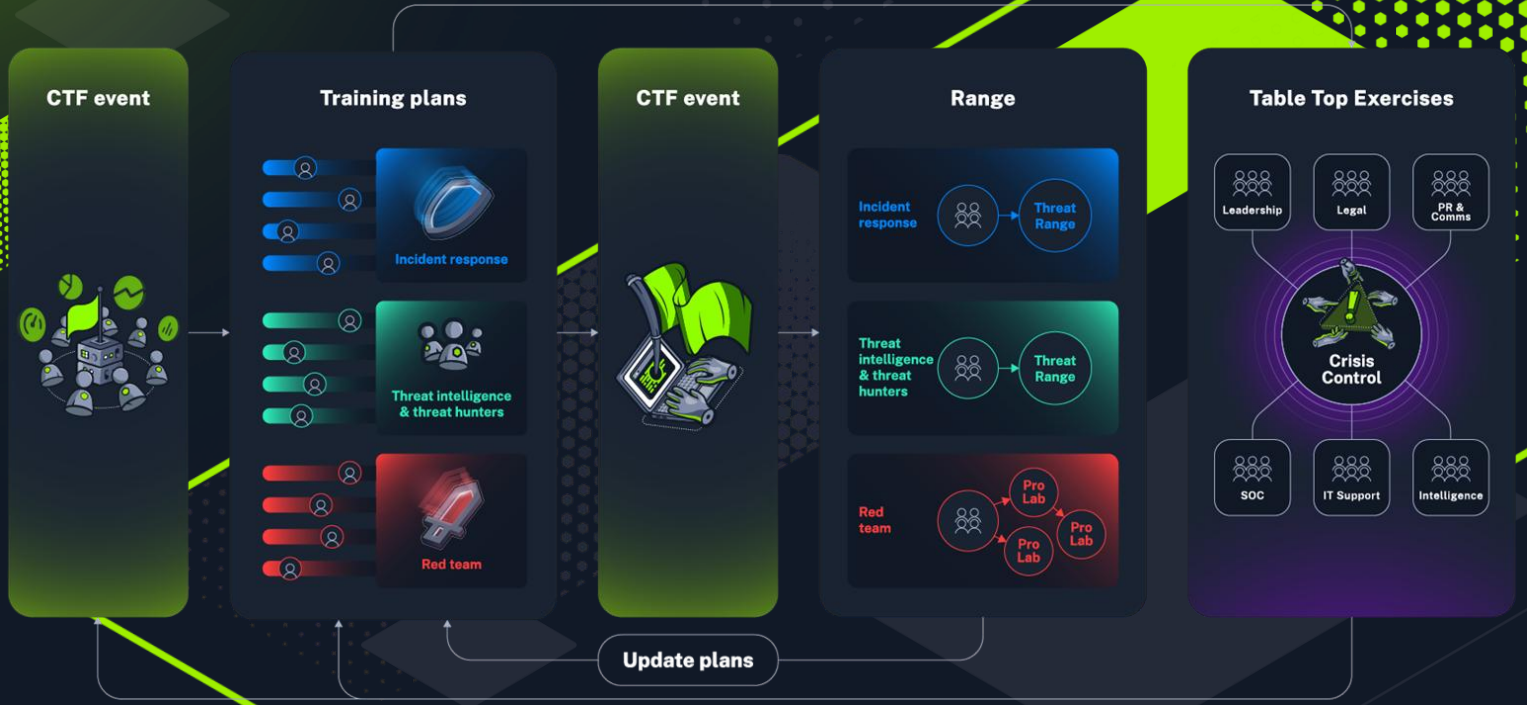
Πλάνο ανάπτυξης δεξιοτήτων ανθρώπινου δυναμικού

Συνεχής προσαρμογή και ανανέωση του εκπαιδευτικού περιεχομένου

Τακτικές αξιολογήσεις και δράσεις benchmarking

Τι κάνουμε διαφορετικά

Ένα οικοσύστημα προϊόντων

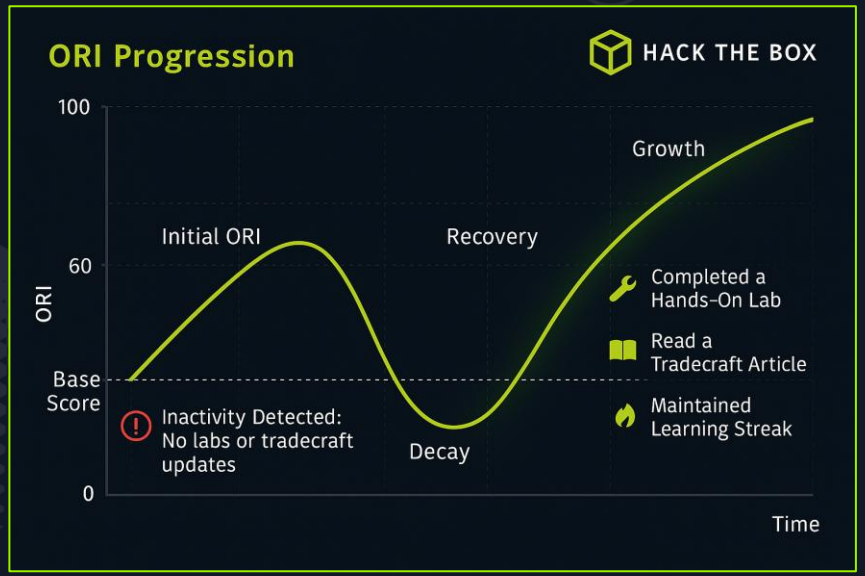


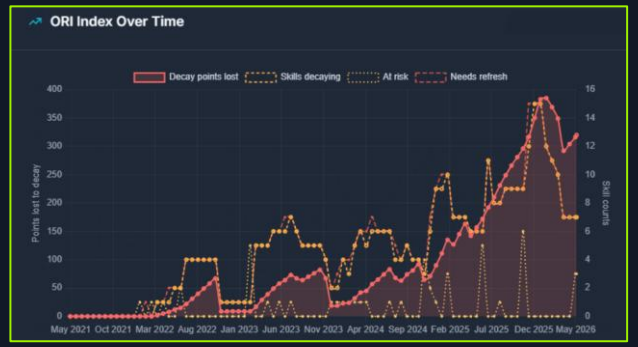
Τι κάνουμε διαφορετικά

Ρεαλιστικά περιβάλλοντα εκπαίδευσης

Τι κάνουμε διαφορετικά

Δείκτης Επιχειρησιακής Ετοιμότητας





GenAI & Το μέλλον

Μια νέα επιφάνεια επίθεσης

{ }

Αμεση Εισχώρηση Εντολών & Διαρροή System Prompt

Κρυφοί κανόνες, κλειδιά και τα συστήματα στα οποία φτάνει το bot εξάγονται κατευθείαν από το context.

!

Jailbreaks & Παράκαμψη Guardrail

Roleplay, obfuscation και persona tricks οδηγούν το μοντέλο πέρα από την πολιτική ασφαλείας του, σε μη επιτρεπτή ή επιβλαβή έξοδο.

@

Διαρροή PII & Ευαίσθητων Δεδομένων

Το bot αναδεικνύει προσωπικά ή ιδιόκτητα δεδομένα από το context, αποθήκες RAG ή μνήμη προηγούμενων γύρων που δεν θα έπρεπε να εκθέσει.

$

Υπερβολική Χρήση Token

Εχθρικά ή επαναλαμβανόμενα prompts διογκώνουν το κόστος inference και εξαντλούν τα rate limits - η διαθεσιμότητα και ο προϋπολογισμός γίνονται ο στόχος.

→

Έμμεση Εισχώρηση Εντολών

Οδηγίες κρυμμένες σε σελίδες, έγγραφα, emails ή έξοδο εργαλείων εκτελούνται όταν το μοντέλο τις απορροφά.

>_

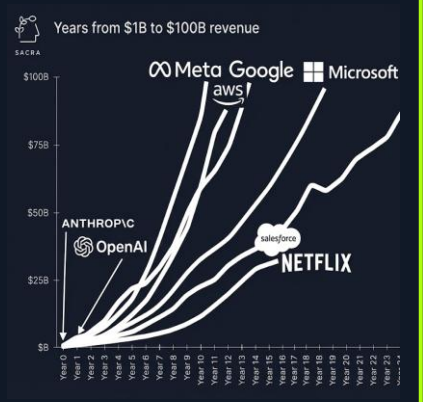
Excessive Agency & Κατάχρηση Εργαλείων

Συνδεδεμένα εργαλεία, βάσεις δεδομένων και APIs μετατρέπουν μία ένεση σε πραγματικές ενέργειες - SSRF, απώλεια δεδομένων, ακούσιες κλήσεις.

GenAI & Το μέλλον

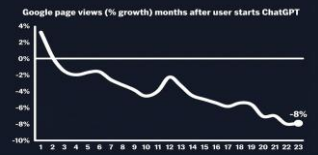
Πιστεύουμε ότι ο κλάδος της κυβερνοασφάλειας βρίσκεται μόλις στην αρχή μιας ταχείας, σαρωτικής επανεφεύρεσης με γνώμονα την AI.

Η GenAI έχει δημιουργήσει τις ταχύτερα αναπτυσσόμενες εταιρείες στην ιστορία…

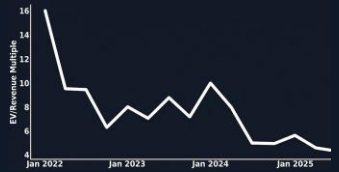


…ανατρέποντας ολόκληρους κλάδους μέσα σε 2-3 χρόνια.

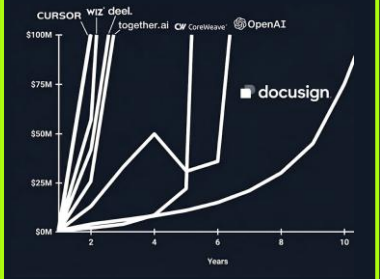
Example 1: Google Search
Declining page views



Example 2: RPA
UIPath declining revenue multiple



Οι προγραμματιστές ήταν οι πρώτοι που την υιοθέτησαν στον επιχειρηματικό χώρο…



Εταιρείες AI όπως οι Cursor και Lovable, φτιαγμένες για παραγωγή κώδικα με AI, φτάνουν σε ορόσημα ετήσιων επαναλαμβανόμενων εσόδων (ARR) 100 εκατ. δολαρίων μέσα σε λίγα χρόνια — και σε χρόνο μόλις 8 μηνών.

…και η κυβερνοασφάλεια είναι η επόμενη.

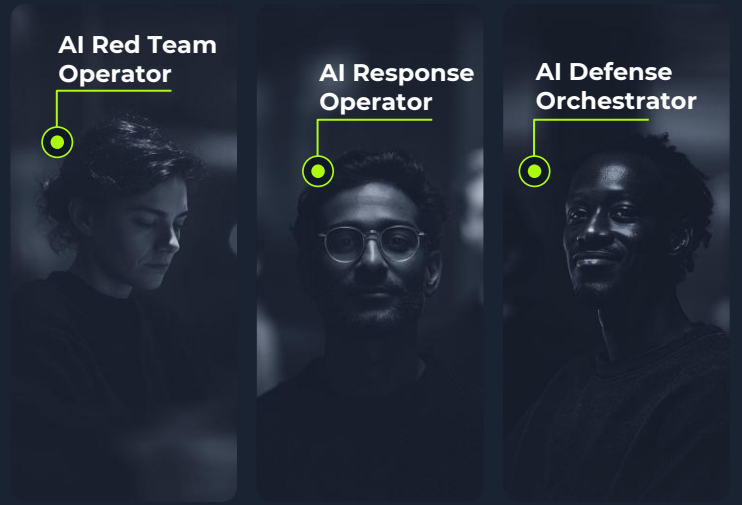
Οι ρόλοι του αύριο

Τι ποσοστό των σημερινών ρόλων μπορεί να ενισχυθεί με την χρήση AI

Οι ρόλοι του αύριο

Οι cyber ρολοι **σημερα**

Οι cyber ρολοι **αυριο**



Οι ρόλοι του αύριο

Οι ρόλοι του αύριο

Υπάρχουν τρία ώριμα πεδία. Καθένα μετρά κάτι υπαρκτό — αλλά κανένα δεν μετρά την ικανοτητα του χειριστή.

ΑΞΙΟΛΟΓΗΣΗ AGENT

Βαθμολογεί τον agent

Αντιστοίχιση τροχιάς, ακρίβεια χρήσης εργαλείων, process reward.

Πλούσιες, δοκιμασμένες μέθοδοι — αλλά το υποκείμενο είναι το μοντέλο, όχι το άτομο που το χειρίζεται.

ΕΠΙΣΤΗΜΗ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ

Βαθμολογεί μεμονωμένες αποφάσεις

Το αν ένας άνθρωπος εμπιστεύτηκε κατάλληλα μία συμβουλή AI.

Στέρεη — αλλά μόνο για μεμονωμένες, ναι/όχι κρίσεις. Ποτέ ανά άτομο, ποτέ σε μια ολόκληρη εργασία.

ΨΥΧΟΜΕΤΡΙΑ

Βαθμολογεί την ικανότητα

Το adaptive testing μετατρέπει τη συμπεριφορά σε μια τεκμηριώσιμη βαθμολογία ικανότητας.

Ώριμη — αλλά ποτέ δεν στράφηκε στο ίχνος αλληλεπίδρασης ανθρώπου-AI.

θ

ΤΟ ΚΕΝΟ → AI-AUGMENTED OPERATOR COMPETENCE (AAOC)

Μια βαθμολογία προερχόμενη από τηλεμετρία και επικυρωμένη, για το πόσο καλά ένα άτομο κατευθύνει έναν αυτόνομο agent σε μια ολόκληρη ανάθεση.

Οι ρόλοι του αύριο

Τα KPIs που εξηγούν τον βαθμό ικανότητας του χειριστή.

1

Κόστος ανά Επαληθευμένο Στόχο

`$ / στόχο`

Συνδέει τη δαπάνη με πραγματικά, επιβεβαιωμένα αποτελέσματα, όχι με ακατέργαστη δραστηριότητα ή πλήθος token.

2

Κατάλληλη Εμπιστοσύνη

`agent / (agent + χειριστής)`

Έπιασε τον agent όταν έκανε λάθος, τον άφησε να τρέξει όταν είχε δίκιο - βαθμολογείται βάσει seeded ground truth

3

Ολοκλήρωση Επαληθευμένη με Κατανόηση

`δικαιολογημένα / ολοκληρωμένα`

Το ποσοστό των ολοκληρωμένων στόχων που ο εκπαιδευόμενος μπορεί πράγματι να δικαιολογήσει - ολοκλήρωση που κατανόησε, όχι απλώς έφτασε. (βασισμένο σε LLM-judge)

Κορυφαίες ομάδες παγκοσμίως εμπιστεύονται την Hack The Box

Δημόσιος τομέας / Κυβερνητικοί οργανισμοί

City of Newcastle

INTER-AMERICAN DEFENSE BOARD

Χρηματοοικονομικές υπηρεσίες

standard chartered

State Farm

Τεχνολογία και συμβουλευτικές υπηρεσίες

pwc

RTX

Google

AUTODESK

securitymetrics

SIEMENS

NTT Security Holdings

BOOKING HOLDINGS

Synack

verizon

SecurityRisk ADVISORS

Άλλοι τομείς

c spire

EA SPORTS

EMERSON

Lufthansa

TOYOTA

Εκπαίδευση

ASU Arizona State University

University of South Florida

NOVI UNIVERSITY OF APPLIED SCIENCES

UNIVERSITY OF SAN FRANCISCO

Drexel University

Sheffield Hallam University Knowledge Applied

CHARLOTTE

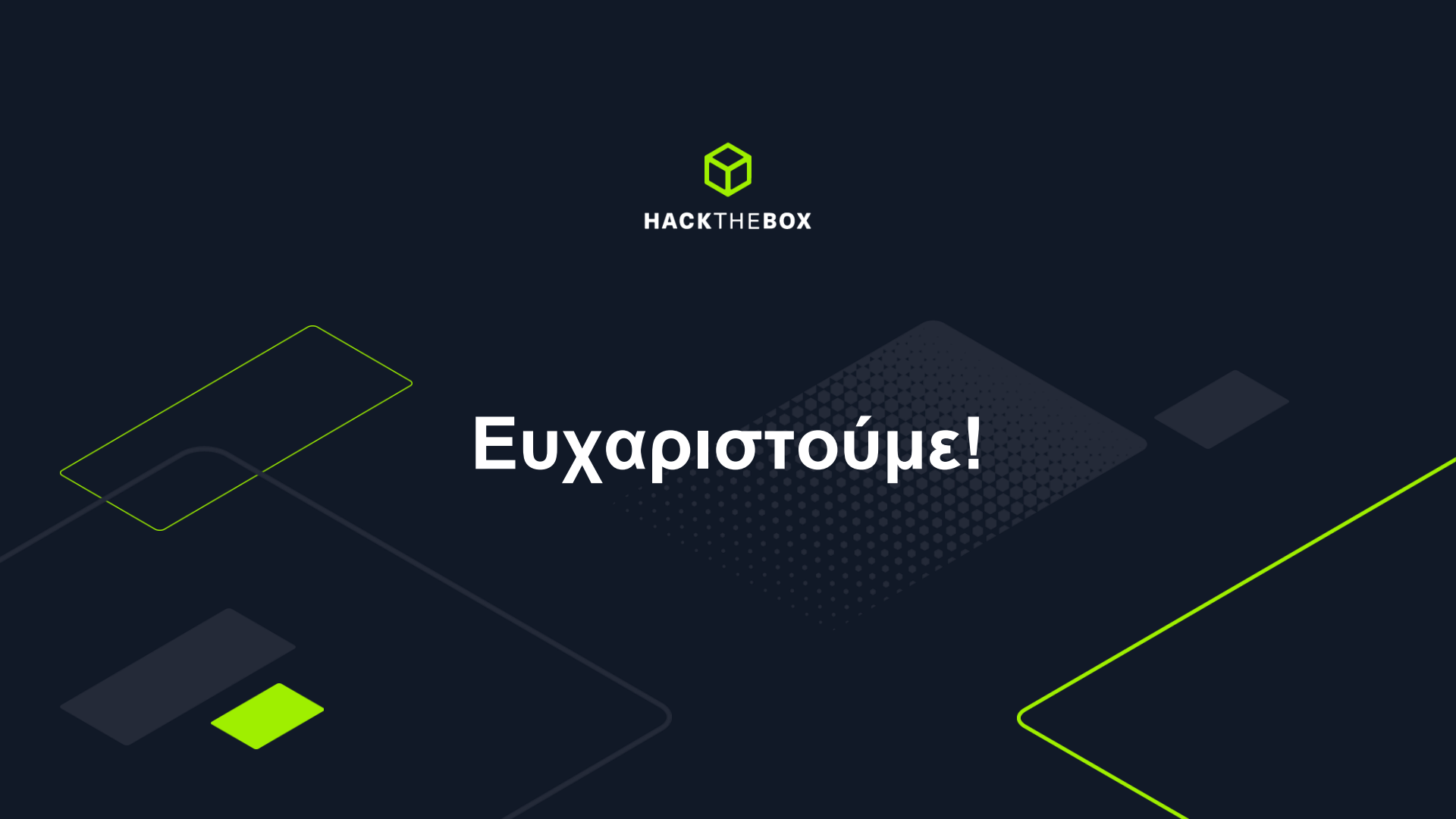
Lancaster University

PURDUE UNIVERSITY

Drake University

NYU

University of BRISTOL



Ευχαριστούμε!