EXTERNAL EXPOSURE BASELINE

Αναφορά Εξωτερικής Ψηφιακής Έκθεσης

Τι βλέπει ένας επιτιθέμενος πριν επιχειρήσει να παραβιάσει τον οργανισμό σας.

ΔΕΙΓΜΑ ΑΝΑΦΟΡΑΣ

Ανώνυμο υπόδειγμα με ενδεικτικά δεδομένα.
Δεν αφορά πραγματικό οργανισμό ή πελάτη.

ΟΡΓΑΝΙΣΜΌΣ	Ανώνυμο δείγμα — εταιρεία 250 εργαζομένων
ΠΑΚΈΤΟ	Baseline Advanced
ΠΕΔΊΟ	3 κύρια domains · 74 επιβεβαιωμένα assets
ΔΙΆΡΚΕΙΑ	5 εργάσιμες ημέρες
ΈΚΔΟΣΗ	Υπόδειγμα v1.0

Audax Cybersecurity · audax.gr · info@audax.gr · +30 210 9839367

Human-led. Machine-scaled. Technically proven.

Σχετικά με αυτό το έγγραφο

Πρόκειται για ανώνυμο υπόδειγμα

Το παρόν είναι δείγμα παραδοτέου της υπηρεσίας Audax External Exposure Baseline. Όλα τα ονόματα, domains, διευθύνσεις και ευρήματα είναι ενδεικτικά και κατασκευασμένα για σκοπούς παρουσίασης. Δεν αφορούν πραγματικό οργανισμό, πραγματικό πελάτη ή πραγματικό περιστατικό. Σκοπός του είναι να δείξει τη δομή, το βάθος και τη γλώσσα της αναφοράς που παραλαμβάνει ο πελάτης.

Τι θα δείτε στις επόμενες σελίδες

- Τη σύνοψη για τη διοίκηση και το Exposure Score, με τεκμηριωμένη μεθοδολογία υπολογισμού.
- Το πεδίο εφαρμογής και — εξίσου σημαντικό — τα ρητά όρια της υπηρεσίας.
- Τη χαρτογράφηση της εξωτερικής επιφάνειας επίθεσης.
- Επιβεβαιωμένα ευρήματα με τεκμήριο, επιχειρησιακό αντίκτυπο και συγκεκριμένη αποκατάσταση.
- Πιθανές διαδρομές επίθεσης, όπως θα τις προσέγγιζε ένας εξωτερικός επιτιθέμενος.
- Τις 10 προτεραιότητες και το πλάνο ενεργειών 30/60/90 ημερών.

Η ουσιαστική διαφορά

Ένα αυτοματοποιημένο εργαλείο παράγει κατάλογο ευρημάτων. Η αναφορά αυτή παράγει κατάλογο αποφάσεων. Κάθε εύρημα έχει περάσει από ανθρώπινη επιβεβαίωση από offensive-security operator, έχει αφαιρεθεί ό,τι δεν επιβεβαιώθηκε, και ό,τι παραμένει συνδέεται με συγκεκριμένο επιχειρησιακό αντίκτυπο και συγκεκριμένη ενέργεια.

Σύνοψη για τη Διοίκηση

62

Executive Exposure Score: 62 / 100 — Αυξημένη έκθεση

Ο οργανισμός διατηρεί σημαντικό αριθμό assets εκτεθειμένων στο Internet τα οποία δεν παρακολουθούνται ενεργά. Δύο εξ αυτών αποτελούν ρεαλιστικά σημεία εκκίνησης επίθεσης. Η εικόνα είναι διορθώσιμη εντός 30–60 ημερών με στοχευμένες ενέργειες.

Η εικόνα με μια ματιά

Δείκτης	Αποτέλεσμα	Σχόλιο
Επιβεβαιωμένα Internet-facing assets	**74**	Έναντι 41 που ήταν γνωστά στην ομάδα IT
Assets εκτός επίσημου καταλόγου	**33**	Κυρίως παλαιά subdomains και staging περιβάλλοντα
Επιβεβαιωμένα ευρήματα	**18**	Από 226 αρχικές ενδείξεις μετά από ανθρώπινη επιβεβαίωση
Κρίσιμα / Υψηλά	**2 / 5**	Απαιτούν ενέργεια εντός 30 ημερών
Πιθανές αρχικές διαδρομές επίθεσης	**2**	Και οι δύο ξεκινούν από μη παρακολουθούμενα assets
Εταιρικοί λογαριασμοί σε γνωστές διαρροές	**31**	Σε 4 διακριτά περιστατικά τρίτων μερών

Τα τρία σημεία που πρέπει να γνωρίζει η διοίκηση

1. Η πραγματική επιφάνεια επίθεσης είναι κατά 80% μεγαλύτερη από την καταγεγραμμένη. Εντοπίστηκαν 74 ενεργά assets έναντι 41 γνωστών. Η διαφορά δεν είναι λογιστική: τα περισσότερα από τα άγνωστα assets δεν καλύπτονται από διαδικασίες ενημερώσεων ή παρακολούθησης.

2. Δύο ευρήματα αποτελούν ρεαλιστικό σημείο εκκίνησης επίθεσης. Ένα περιβάλλον δοκιμών με ενεργό πίνακα διαχείρισης και ένα σημείο απομακρυσμένης πρόσβασης χωρίς δεύτερο παράγοντα ταυτοποίησης. Και τα δύο είναι διορθώσιμα άμεσα.

3. Το πρόβλημα είναι διαρκές, όχι στιγμιαίο. Τα 33 άγνωστα assets δεν δημιουργήθηκαν σε μία ημέρα· συσσωρεύτηκαν. Χωρίς συνεχή παρακολούθηση, η ίδια απόκλιση θα έχει επανεμφανιστεί εντός 12 μηνών.

Η σύσταση σε μία πρόταση

Άμεση αποκατάσταση των 7 ευρημάτων Κρίσιμης και Υψηλής σοβαρότητας εντός 30 ημερών, απόσυρση ή ένταξη των 33 μη καταγεγραμμένων assets σε επίσημη διαχείριση εντός 60 ημερών, και θέσπιση συνεχούς παρακολούθησης της εξωτερικής έκθεσης ώστε η εικόνα να μην επιδεινωθεί ξανά.

Πεδίο Εφαρμογής & Μεθοδολογία

Τι περιλαμβάνει η αξιολόγηση

Φάση	Περιεχόμενο
1. Παθητική αναγνώριση	Χαρτογράφηση domains, subdomains, IP εύρους, πιστοποιητικών, DNS εγγραφών και δημόσια διαθέσιμων πληροφοριών, χωρίς καμία αλληλεπίδραση με τα συστήματα του οργανισμού.
2. Έγκριση πεδίου	Ο κατάλογος των assets που εντοπίστηκαν υποβάλλεται στον πελάτη. Καμία ενεργητική ενέργεια δεν εκτελείται πριν από γραπτή έγκριση του πεδίου.
3. Ελεγχόμενη επαλήθευση	Επιβεβαίωση ενεργών υπηρεσιών, τεχνολογιών και ρυθμίσεων με ρυθμό περιορισμένης έντασης, ώστε να μην επηρεαστεί η διαθεσιμότητα των παραγωγικών συστημάτων.
4. Ανθρώπινη επιβεβαίωση	Κάθε ένδειξη αξιολογείται από offensive-security operator. Απορρίπτονται τα μη επιβεβαιωμένα ευρήματα και ιεραρχείται ό,τι απομένει βάσει πραγματικής εκμεταλλευσιμότητας.
5. Τεκμηρίωση	Σύνταξη τεχνικής και διοικητικής αναφοράς, πλάνου προτεραιοτήτων και παρουσίαση αποτελεσμάτων στα εμπλεκόμενα μέρη.

Τι ΔΕΝ είναι η υπηρεσία

Η σαφήνεια εδώ προστατεύει και τις δύο πλευρές. Το External Exposure Baseline:

- δεν είναι πλήρες penetration test και δεν το υποκαθιστά·
- δεν περιλαμβάνει ανεξέλεγκτη εκμετάλλευση ευπαθειών·
- δεν περιλαμβάνει επιθέσεις σε συνθηματικά (brute force, password spraying)·
- δεν εξετάζει την εσωτερική υποδομή του οργανισμού·
- δεν υποκαθιστά Red Team ή εξειδικευμένο έλεγχο εφαρμογών·
- δεν παραδίδει αυτοματοποιημένα αποτελέσματα χωρίς ανθρώπινη επιβεβαίωση.

Όταν ένα εύρημα απαιτεί βαθύτερη επαλήθευση ή απόδειξη εκμεταλλευσιμότητας, το αποτέλεσμα του Baseline μετατρέπεται σε συγκεκριμένο, τεκμηριωμένο πεδίο για penetration testing — χωρίς να χρεώνεται εκ νέου η φάση αναγνώρισης.

> **Εξουσιοδότηση**
> Καμία ενέργεια δεν εκτελείται χωρίς υπογεγραμμένη εξουσιοδότηση ελέγχου και επαλήθευση ότι ο οργανισμός ελέγχει πράγματι τα domains που δηλώνει. Η επαλήθευση γίνεται μέσω εγγραφής DNS πριν την έναρξη οποιασδήποτε δραστηριότητας.

Πώς Υπολογίζεται το Exposure Score

Το Exposure Score δεν είναι αυθαίρετος αριθμός ούτε προϊόν εργαλείου. Υπολογίζεται από πέντε μετρήσιμους άξονες, με σταθερή στάθμιση που παραμένει ίδια σε κάθε αξιολόγηση και σε κάθε επανέλεγχο — ώστε τα αποτελέσματα να είναι συγκρίσιμα διαχρονικά.

Άξονας	Τι μετρά	Βάρος	Δείγμα
Ορατότητα	Ποσοστό assets εκτός επίσημου καταλόγου	**25%**	18 / 25
Εκμεταλλευσιμότητα	Ευρήματα με ρεαλιστική διαδρομή αρχικής πρόσβασης	**30%**	19 / 30
Ρυθμίσεις	DNS, TLS, email authentication, security headers	**20%**	11 / 20
Έκθεση ταυτοτήτων	Εταιρικοί λογαριασμοί σε γνωστές διαρροές	**15%**	9 / 15
Ωριμότητα	Ύπαρξη διαδικασιών παρακολούθησης και απόσυρσης assets	**10%**	5 / 10
Σύνολο		**100%**	**62 / 100**

Ερμηνεία κλίμακας

0–25	Ελεγχόμενη έκθεση — η επιφάνεια επίθεσης είναι γνωστή και διαχειρίσιμη.
26–50	Περιορισμένη έκθεση — υπάρχουν κενά, χωρίς άμεσα εκμεταλλεύσιμα σημεία.
51–75	Αυξημένη έκθεση — υπάρχουν ρεαλιστικά σημεία εκκίνησης επίθεσης.
76–100	Κρίσιμη έκθεση — άμεση προτεραιότητα αποκατάστασης.

Υψηλότερη βαθμολογία σημαίνει μεγαλύτερη έκθεση. Σε επανέλεγχο, η μεταβολή του σκορ αποτυπώνει την πραγματική βελτίωση και μπορεί να χρησιμοποιηθεί ως δείκτης προόδου προς τη διοίκηση.

Εξωτερική Επιφάνεια Επίθεσης

Σύνοψη ανά κατηγορία

Κατηγορία	Εντοπίστηκαν	Γνωστά στον οργανισμό	Παρατήρηση
Κύρια domains	**3**	3	Πλήρης αντιστοίχιση
Ενεργά subdomains	**48**	22	26 εκτός καταλόγου
Δημόσιες IP διευθύνσεις	**11**	9	2 σε πάροχο cloud
Εφαρμογές web	**19**	12	3 περιβάλλοντα δοκιμών
Σημεία απομακρυσμένης πρόσβασης	**4**	3	1 χωρίς δεύτερο παράγοντα
Πίνακες διαχείρισης	**5**	1	4 προσβάσιμοι δημόσια
Υπηρεσίες τρίτων	**7**	4	Κυρίως SaaS με εταιρικό branding

Ενδεικτικό απόσπασμα καταλόγου assets

Στην πλήρη αναφορά ο κατάλογος παραδίδεται και σε μορφή υπολογιστικού φύλλου, με όλα τα πεδία ανά asset (τεχνολογία, πιστοποιητικό, τελευταία μεταβολή, ιδιοκτήτης).

Asset	Τύπος	Κατάσταση	Σημείωση
`vpn.[redacted].gr`	Remote access	Ενεργό	Χωρίς δεύτερο παράγοντα
`staging.[redacted].gr`	Web / δοκιμές	Ενεργό	Εκτεθειμένος πίνακας διαχείρισης
`old-portal.[redacted].gr`	Web	Ενεργό	Εκτός καταλόγου από το 2023
`mail.[redacted].gr`	Email	Ενεργό	Ελλιπής πολιτική DMARC
`cdn-assets.[redacted].gr`	Cloud storage	Ενεργό	Δημόσια αναγνώσιμο
`legacy-api.[redacted].gr`	API	Ενεργό	Παρωχημένη έκδοση βιβλιοθήκης

Επιβεβαιωμένα Ευρήματα

Από 226 αρχικές ενδείξεις, 18 επιβεβαιώθηκαν από operator. Ακολουθεί ενδεικτικό απόσπασμα· στην πλήρη αναφορά κάθε εύρημα συνοδεύεται από τεκμήριο (screenshot, απόκριση υπηρεσίας) και αναφορές σε αντίστοιχα πρότυπα.

F-01	Περιβάλλον δοκιμών με προσβάσιμο πίνακα διαχείρισης	Κρίσιμο
Asset	staging.[redacted].gr	
Εύρημα	Περιβάλλον δοκιμών προσβάσιμο από το Internet, με ενεργό πίνακα διαχείρισης και προεπιλεγμένη σελίδα σύνδεσης. Το περιβάλλον περιέχει αντίγραφο της παραγωγικής εφαρμογής.	
Επιχειρησιακός αντίκτυπος	Ένας επιτιθέμενος αποκτά γνώση της εφαρμογής και πιθανό σημείο εισόδου, χωρίς να χρειαστεί να αγγίξει το παραγωγικό σύστημα. Τυχόν δεδομένα δοκιμών προερχόμενα από παραγωγή συνιστούν επιπλέον έκθεση.	
Αποκατάσταση	Απόσυρση του περιβάλλοντος ή περιορισμός πρόσβασης σε συγκεκριμένα δίκτυα. Εφόσον απαιτείται εξωτερική πρόσβαση, ένταξη πίσω από ταυτοποίηση και αφαίρεση κάθε δεδομένου παραγωγής.	

F-02	Σημείο απομακρυσμένης πρόσβασης χωρίς δεύτερο παράγοντα	Κρίσιμο
Asset	vpn.[redacted].gr	
Εύρημα	Το σημείο απομακρυσμένης πρόσβασης δέχεται ταυτοποίηση με συνθηματικό μόνο. Εντοπίστηκαν εταιρικές διευθύνσεις του ίδιου domain σε γνωστές διαρροές τρίτων.	
Επιχειρησιακός αντίκτυπος	Ο συνδυασμός εκτεθειμένων ταυτοτήτων και απουσίας δεύτερου παράγοντα αποτελεί την συχνότερη διαδρομή αρχικής πρόσβασης σε περιστατικά ransomware.	
Αποκατάσταση	Άμεση ενεργοποίηση δεύτερου παράγοντα ταυτοποίησης, κατά προτίμηση ανθεκτικού σε phishing. Υποχρεωτική αλλαγή συνθηματικών για τους λογαριασμούς που εντοπίστηκαν σε διαρροές.	

F-03	Ελλιπής πολιτική ταυτοποίησης εξερχόμενης αλληλογραφίας	Υψηλό
Asset	[redacted].gr (DNS / DMARC)	
Εύρημα	Η πολιτική DMARC βρίσκεται σε κατάσταση παρακολούθησης χωρίς εφαρμογή, ενώ μία εγγραφή SPF περιλαμβάνει παρωχημένο πάροχο που δεν χρησιμοποιείται πλέον.	
Επιχειρησιακός αντίκτυπος	Επιτρέπεται η πλαστογράφηση της εταιρικής αλληλογραφίας προς πελάτες και συνεργάτες — συνήθης αφετηρία απάτης τύπου BEC και στοχευμένου phishing.	
Αποκατάσταση	Καθαρισμός εγγραφών SPF, σταδιακή μετάβαση της πολιτικής DMARC σε εφαρμογή, παρακολούθηση αναφορών για 30 ημέρες πριν την πλήρη ενεργοποίηση.	

F-04	Παλαιά εφαρμογή εκτός κύκλου συντήρησης	Υψηλό
Asset	old-portal.[redacted].gr	
Εύρημα	Ενεργή εφαρμογή που δεν περιλαμβάνεται στον κατάλογο συστημάτων και δεν έχει λάβει ενημερώσεις. Η έκδοση της υποκείμενης πλατφόρμας έχει γνωστές δημοσιευμένες ευπάθειες.	
Επιχειρησιακός αντίκτυπος	Ένα σύστημα που κανείς δεν παρακολουθεί δεν πρόκειται να ενημερωθεί ούτε να ελεγχθεί. Αποτελεί μόνιμο σημείο κινδύνου με μηδενική ορατότητα.	
Αποκατάσταση	Απόσυρση εφόσον δεν εξυπηρετεί λειτουργική ανάγκη. Διαφορετικά, ένταξη στον επίσημο κατάλογο, ενημέρωση και υπαγωγή στη διαδικασία διαχείρισης ευπαθειών.	

F-05	Δημόσια αναγνώσιμος αποθηκευτικός χώρος	Μεσαίο
Asset	cdn-assets.[redacted].gr	
Εύρημα	Χώρος αποθήκευσης σε πάροχο cloud με δημόσια δικαιώματα ανάγνωσης και δυνατότητα καταλογογράφησης περιεχομένου.	
Επιχειρησιακός αντίκτυπος	Έκθεση εσωτερικών εγγράφων ή αρχείων που δεν προορίζονταν για δημοσίευση· δυνατότητα συλλογής πληροφοριών για επόμενα στάδια επίθεσης.	
Αποκατάσταση	Απενεργοποίηση καταλογογράφησης, περιορισμός δικαιωμάτων ανάγνωσης, έλεγχος του υφιστάμενου περιεχομένου για ευαίσθητα αρχεία.	

Πιθανές Διαδρομές Επίθεσης

Οι διαδρομές που ακολουθούν περιγράφουν πώς θα μπορούσε να συνδυαστεί ένα σύνολο ευρημάτων. Δεν εκτελέστηκαν — η επιβεβαίωση εκμεταλλευσιμότητας απαιτεί penetration testing με διακριτό πεδίο και εξουσιοδότηση.

Διαδρομή Α — Απομακρυσμένη πρόσβαση μέσω εκτεθειμένων ταυτοτήτων

1	Συλλογή εταιρικών διευθύνσεων από δημόσιες πηγές και γνωστές διαρροές τρίτων.
2	Αντιστοίχιση με το σημείο απομακρυσμένης πρόσβασης (F-02), το οποίο δέχεται μόνο συνθηματικό.
3	Απόπειρα σύνδεσης με ήδη εκτεθειμένα διαπιστευτήρια.
4	Πρόσβαση σε εσωτερικούς πόρους με τα δικαιώματα του χρήστη.

Σημείο διακοπής: η ενεργοποίηση δεύτερου παράγοντα ταυτοποίησης ακυρώνει τη διαδρομή στο βήμα 3.

Διαδρομή Β — Από το περιβάλλον δοκιμών στη γνώση της παραγωγής

1	Εντοπισμός του περιβάλλοντος δοκιμών (F-01) μέσω δημόσιων πιστοποιητικών.
2	Πρόσβαση στον πίνακα διαχείρισης και χαρτογράφηση της εφαρμογής.
3	Άντληση πληροφοριών για δομή, τελικά σημεία και τεχνολογίες παραγωγής.
4	Στοχευμένη επίθεση στο παραγωγικό σύστημα με γνώση που δεν θα ήταν διαθέσιμη.

Σημείο διακοπής: ο περιορισμός πρόσβασης στο περιβάλλον δοκιμών ακυρώνει τη διαδρομή στο βήμα 2.

Οι 10 Προτεραιότητες Αποκατάστασης

Η ιεράρχηση γίνεται με βάση τη μείωση πραγματικού κινδύνου ανά μονάδα προσπάθειας — όχι με βάση τη βαθμολογία ενός εργαλείου.

#	Ενέργεια	Σοβαρότητα	Προσπάθεια
1	Ενεργοποίηση δεύτερου παράγοντα στην απομακρυσμένη πρόσβαση	Κρίσιμο	Χαμηλή
2	Απόσυρση ή περιορισμός του περιβάλλοντος δοκιμών	Κρίσιμο	Χαμηλή
3	Αλλαγή συνθηματικών για τους λογαριασμούς σε διαρροές	Υψηλό	Χαμηλή
4	Περιορισμός πρόσβασης στους 4 δημόσιους πίνακες διαχείρισης	Υψηλό	Χαμηλή
5	Απόσυρση της παλαιάς εφαρμογής εκτός συντήρησης	Υψηλό	Μεσαία
6	Καθαρισμός SPF και μετάβαση DMARC σε εφαρμογή	Υψηλό	Μεσαία
7	Περιορισμός δικαιωμάτων στον αποθηκευτικό χώρο cloud	Μεσαίο	Χαμηλή
8	Ανανέωση πιστοποιητικών και απόσυρση παρωχημένων πρωτοκόλλων	Μεσαίο	Μεσαία
9	Ένταξη των 33 άγνωστων assets σε επίσημο κατάλογο	Μεσαίο	Υψηλή
10	Θέσπιση διαδικασίας απόσυρσης assets στο τέλος ζωής	Χαμηλό	Μεσαία

Πλάνο Ενεργειών 30 / 60 / 90 Ημερών

Ορίζοντας	Στόχος	Ενέργειες
0–30 ημέρες	Κλείσιμο των ρεαλιστικών σημείων εισόδου	Προτεραιότητες 1–4. Στοχευμένη, χαμηλής προσπάθειας παρέμβαση με τη μεγαλύτερη μείωση κινδύνου.
31–60 ημέρες	Εξυγίανση της επιφάνειας επίθεσης	Προτεραιότητες 5–8. Απόσυρση παλαιών συστημάτων και διόρθωση ρυθμίσεων.
61–90 ημέρες	Θεσμοθέτηση ελέγχου	Προτεραιότητες 9–10 και επανέλεγχος για επιβεβαίωση της βελτίωσης με νέο Exposure Score.

Επόμενα Βήματα

Μετά την παράδοση της αναφοράς ο οργανισμός έχει τρεις δρόμους. Δεν είναι αμοιβαία αποκλειστικοί και δεν υπάρχει πίεση για κανέναν.

Επιλογή Α — Αποκατάσταση με ίδια μέσα

Ο οργανισμός παραλαμβάνει την αναφορά, τον κατάλογο assets και το πλάνο 30/60/90 και υλοποιεί τις διορθώσεις με τη δική του ομάδα. Το παραδοτέο είναι πλήρες και αυτοτελές.

Επιλογή Β — Penetration Testing

Όπου απαιτείται απόδειξη ότι μια διαδρομή επίθεσης είναι πράγματι εκμεταλλεύσιμη, η Audax εκτελεί στοχευμένο penetration test. Το πεδίο προκύπτει από τα ευρήματα του Baseline, επομένως δεν χρεώνεται εκ νέου η φάση αναγνώρισης.

Επιλογή Γ — Συνεχής παρακολούθηση με το Erevos AI

Η εικόνα που αποτυπώνει αυτή η αναφορά ισχύει για σήμερα. Με το Erevos AI — την ετήσια υπηρεσία συνεχούς διαχείρισης έκθεσης της Audax — παρακολουθούνται διαρκώς τα νέα assets, οι μεταβολές στην επιφάνεια επίθεσης, η πρόοδος αποκατάστασης και η τυχόν επανεμφάνιση προβλημάτων.

Εμπορικοί όροι μετάβασης

Το 50% της αξίας του Exposure Baseline συμψηφίζεται με το πρώτο ετήσιο συμβόλαιο Erevos AI, εφόσον αυτό υπογραφεί εντός 30 ημερών από την παράδοση της αναφοράς. Για ετήσιες συμβάσεις άνω των 24.000 € συμψηφίζεται ολόκληρη η αξία του Baseline. Οι όροι επιβεβαιώνονται γραπτώς στην προσφορά.

Περιορισμοί και ισχύς της αναφοράς

Η αξιολόγηση αποτυπώνει την εξωτερική έκθεση του οργανισμού κατά τη χρονική περίοδο εκτέλεσής της. Η επιφάνεια επίθεσης μεταβάλλεται με κάθε νέα υπηρεσία, εφαρμογή ή αλλαγή υποδομής. Η απουσία ενός ευρήματος δεν συνιστά βεβαίωση ασφάλειας, ούτε η αναφορά αποτελεί πιστοποίηση συμμόρφωσης. Τα αποτελέσματα προορίζονται αποκλειστικά για τον οργανισμό-αποδέκτη.

Ζητήστε το δικό σας Exposure Baseline

Παράδοση σε 5 εργάσιμες ημέρες. Πακέτα από 1.500 € + ΦΠΑ, με ταχύ έλεγχο ενός domain από 490 € + ΦΠΑ.

audax.gr/external-exposure-baseline/ · info@audax.gr · +30 210 9839367