ΔΙΚΗΓΟΡΙΚΟΣ ΣΥΛΛΟΓΟΣ ΑΘΗΝΩΝ

Ακαδημίας 60 – Τ.Κ. 10679
Τηλ.: 210-3398182

ΑΝΑΡΤΗΤΕΑ

ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Αθήνα, 16/6/2026
Αρ. πρωτ: 4638

ΕΠΑΝΑΠΡΟΚΗΡΥΞΗ ΠΡΟΧΕΙΡΟΥ ΔΙΑΓΩΝΙΣΜΟΥ

ΑΠΟΦΑΣΗ

«ΠΡΟΜΗΘΕΙΑ ΥΠΗΡΕΣΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΟΠΣ ΟΛΟΜΕΛΕΙΑΣ»

ΓΕΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΔΙΑΓΩΝΙΣΜΟΥ

Είδος διαγωνισμού:	Πρόχειρος διαγωνισμός με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά.
Τόπος κατάθεσης προσφορών:	Γραφεία ΔΣΑ, οδός Ακαδημίας αριθ. 60 – Τ.Κ. 10679 Αθήνα (Τμήμα Πρωτοκόλλου 2ος όροφος).
Καταληκτική ημερομηνία και ώρα υποβολής προσφορών:	30/06/2026 ημέρα Τρίτη και ώρα 12:00μμ
Τόπος και Χρόνος διενέργειας του διαγωνισμού - αποσφράγιση προσφορών:	Γραφεία ΔΣΑ, οδός Ακαδημίας αριθ. 60 - ΤΚ 10679 Αθήνα (αίθουσα ΤΑΚΗ ΠΑΠΠΑ) στις 30/06/2026, ημέρα Τρίτη και ώρα 13:00μμ

Αντικείμενο:	Προμήθεια υπηρεσιών διαχείρισης ασφάλειας του ΟΠΣ Ολομέλειας για ένα έτος από την υπογραφή της σύμβασης
Προϋπολογισθείσα δαπάνη **χωρίς ΦΠΑ:** Προϋπολογισθείσα δαπάνη **με ΦΠΑ 24%:**	Τριάντα χιλιάδες (30.000) **€** Τριάντα επτά χιλιάδες διακόσια (37.200) €
Διάρκεια ισχύος προσφορών:	Ενενήντα (90) ημέρες από την επόμενη της διενέργειας του διαγωνισμού.

Ο Δικηγορικός Σύλλογος Αθηνών (ΔΣΑ), αφού έλαβε υπόψη του: τον κανονισμό προμηθειών του, την από 09/06/2026 απόφαση του Διοικητικού Συμβουλίου και τις ανάγκες της υπηρεσίας

ΠΡΟΚΗΡΥΣΣΕΙ

Πρόχειρο διαγωνισμό, με γραπτές σφραγισμένες προσφορές με κριτήριο κατακύρωσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά, για την ανάδειξη αναδόχου για την προμήθεια υπηρεσιών διαχείρισης ασφάλειας του ΟΠΣ Ολομέλειας.

ΠΡΟΫΠΟΛΟΓΙΣΜΟΣ

Η συνολική προϋπολογιζόμενη δαπάνη της ανωτέρω προμήθειας ανέρχεται στο ποσό των τριάντα επτά χιλιάδων διακοσίων (37.200) ευρώ συμπεριλαμβανομένου του αναλογούντος ΦΠΑ 24%.

ΥΠΟΒΟΛΗ ΠΡΟΣΦΟΡΩΝ

Όσοι επιθυμούν να λάβουν μέρος στο διαγωνισμό μπορούν να υποβάλλουν προσφορές, σύμφωνα με τα οριζόμενα στην παρούσα διακήρυξη το αργότερο μέχρι τις 30/06/2026, ημέρα Τρίτη και ώρα 12:00μμ, στα γραφεία του ΔΣΑ, οδός Ακαδημίας αρ. 60 - ΤΚ 10679 Αθήνα (Τμήμα Πρωτοκόλλου 2ος όροφος).

Προσφορές που θα κατατεθούν μετά την παραπάνω ημερομηνία και ώρα, λογίζονται ως εκπρόθεσμες, απορρίπτονται ως απαράδεκτες και επιστρέφονται. Οι συμμετέχοντες υποχρεούνται να υποβάλλουν προσφορά για το σύνολο της προμήθειας. Δε γίνονται δεκτές και απορρίπτονται ως απαράδεκτες, προσφορές που υποβάλλονται για μέρος μόνο της προμήθειας. Η κατακύρωση θα γίνει, με κριτήριο την πλέον συμφέρουσα από οικονομική άποψη προσφορά.

ΤΟΠΟΣ ΚΑΙ ΧΡΟΝΟΣ ΔΙΕΝΕΡΓΕΙΑΣ ΔΙΑΓΩΝΙΣΜΟΥ

Ο διαγωνισμός θα διενεργηθεί στα γραφεία του ΔΣΑ (αίθουσα ΤΑΚΗ ΠΑΠΠΑ) στις 30/06/2026, ημέρα Τρίτη και ώρα 13:00μμ
Αναπόσπαστο μέρος της παρούσας αποτελούν:

ΠΑΡΑΡΤΗΜΑ Α: ΓΕΝΙΚΟΙ ΟΡΟΙ ΔΙΑΓΩΝΙΣΜΟΥ

ΠΑΡΑΡΤΗΜΑ Β : **ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ**

ΠΑΡΑΡΤΗΜΑ Γ : **ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ**

Ο διαγωνισμός θα διεξαχθεί με βάση τους όρους της παρούσας διακήρυξης, όπως αυτοί αναλύονται στα Παραρτήματα Α, Β και Γ αυτής και τις διατάξεις του Κανονισμού Προμηθειών του ΔΣΑ που είναι αναρτημένος στην ιστοσελίδα του ΔΣΑ ,ο οποίος αποτελεί αναπόσπαστο μέρος της παρούσας διακήρυξης Η διακήρυξη αυτή θα αναρτηθεί στην επίσημη ιστοσελίδα του ΔΣΑ (www.dsa.gr)

Ο ΓΕΝΙΚΟΣ ΔΙΕΥΘΥΝΤΗΣ ΤΟΥ ΔΣΑ

ΚΩΝΣΤΑΝΤΙΝΟΣ Δ. ΡΙΖΟΣ

ΠΑΡΑΡΤΗΜΑ Α

ΓΕΝΙΚΟΙ ΟΡΟΙ ΔΙΑΓΩΝΙΣΜΟΥ

1. <u>Δικαίωμα συμμετοχής</u>

1.1.Δικαίωμα συμμετοχής στο διαγωνισμό έχουν:

Φυσικά ή νομικά πρόσωπα καθώς και Ενώσεις / Κοινοπραξίες των ανωτέρω φυσικών ή νομικών προσώπων, που υποβάλλουν κοινή προσφορά.

Οι Ενώσεις / Κοινοπραξίες δεν απαιτείται να έχουν συγκεκριμένη νομική μορφή κατά την υποβολή της προσφοράς. Σε περίπτωση που Ένωση / Κοινοπραξία επιλεγεί είναι δυνατόν να υποχρεωθεί να περιβληθεί σε συγκεκριμένη νομική μορφή, εάν της ανατεθεί η σύμβαση, στο μέτρο που η περιβολή αυτής της νομικής μορφής είναι αναγκαία για την ορθή εκτέλεση της σύμβασης.

Στην προσφορά της Ένωσης /Κοινοπραξίας θα πρέπει να αναγράφεται απαραιτήτως το ποσοστό συμμετοχής κάθε μέλους. Επίσης πρέπει να υποβάλλεται με την προσφορά και το ισχύον συμφωνητικό σύστασης.

1.2. Κάθε συμμετέχων μεμονωμένα ή ως μέλος Ένωσης/ Κοινοπραξίας, πρέπει:

1.2.1. Να μην τελεί σε πτώχευση και σε διαδικασία κήρυξης σε πτώχευση.

1.2.2. Να είναι φορολογικά ενήμερος ως προς τις φορολογικές υποχρεώσεις του και ασφαλιστικά ενήμερος ως προς τις υποχρεώσεις του που αφορούν τις εισφορές κοινωνικής ασφάλισης (κύριας και επικουρικής).

1.2.3. Να μην έχει καταδικαστεί αμετάκλητα για:

α) συμμετοχή σε εγκληματική οργάνωση, κατά το άρθρο 2 παρ.1 της κοινής δράσης της αριθμ. 98/773/ΔΕΥ του Συμβουλίου της Ευρωπαϊκής Ένωσης,

β) δωροδοκία, κατά το άρθρο 3 της πράξης του Συμβουλίου της 26ης Μαΐου 1997 (21) και στο άρθρο 3 παρ.1 της κοινής δράσης αριθμ. 98/742/ΚΕΠΠΑ του Συμβουλίου,

γ) απάτη, κατά την έννοια του άρθρου 1 της σύμβασης για την προστασία των οικονομικών συμφερόντων των Ευρωπαϊκών Κοινοτήτων,

δ) νομιμοποίηση εσόδων από παράνομες δραστηριότητες, κατά το άρθρο 1 της αριθμ. 91/308/ΕΟΚ οδηγίας του Συμβουλίου, για την πρόληψη χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες,

ε) υπεξαίρεση (375 Π.Κ),

στ) απάτη (386-387 Π.Κ.),

ζ) εκβίαση (385 Π.Κ.),

η) πλαστογραφία (216-217 Π.Κ.),

θ) ψευδής κατάθεση (224 Π.Κ.),

ι) δωροδοκία-δωροληψία (235-237 Π.Κ.)

Σε περίπτωση που ο συμμετέχων έχει εταιρική μορφή, οι πιο πάνω προϋποθέσεις πρέπει να συντρέχουν στο πρόσωπο των διαχειριστών σε περίπτωση ομόρρυθμων (ΟΕ), ετερόρρυθμων (ΕΕ) και εταιρειών περιορισμένης ευθύνης (ΕΠΕ) και για τον πρόεδρο, τον διευθύνοντα σύμβουλο ή και τους τυχόν άλλους νομίμους εκπροσώπους της, σε περίπτωση ανώνυμης εταιρείας (ΑΕ).

1.2.4. Σε περίπτωση που ο συμμετέχων έχει εταιρική μορφή, η εταιρία πρέπει επιπλέον να μην τελεί σε αναγκαστική διαχείριση, κοινή ή ειδική εκκαθάριση, διαδικασία εξυγίανσης ή άλλη ανάλογη κατάσταση που δημιουργεί αμφιβολίες, ως προς τη φερεγγυότητα και την οικονομική ευρωστία της, καθώς επίσης να μην τελεί σε διαδικασία κήρυξής της σε μία από τις προαναφερόμενες καταστάσεις.

1.2.5. Ο διαγωνιζόμενος να μην έχει αποκλεισθεί από συμμετοχή σε δημόσιους διαγωνισμούς.

Επισημαίνεται ότι σε περίπτωση υποβολής κοινής προσφοράς, από Ένωση/ Κοινοπραξία, οι παραπάνω λόγοι αποκλεισμού ισχύουν για καθέναν από τους συμμετέχοντες ξεχωριστά στην κοινή προσφορά. Εάν συντρέχει λόγος

αποκλεισμού έστω και για έναν συμμετέχοντα σε κοινή προσφορά, η υποβληθείσα κοινή προσφορά απορρίπτεται ως απαράδεκτη.

Η συνδρομή των παραπάνω προϋποθέσεων αποδεικνύεται από πιστοποιητικά που εκδίδονται από αρμόδιες δικαστικές ή διοικητικές αρχές. Τα πιστοποιητικά αυτά θα υποβληθούν στον ΔΣΑ από τον υποψήφιο ανάδοχο στον οποίο θα κατακυρωθούν τα αποτελέσματα του διαγωνισμού, σύμφωνα με τα αναφερόμενα στον όρο 6 της παρούσης.

2. <u>Κατάρτιση, υποβολή και αποσφράγιση προσφορών.</u>

2.1.Όσοι επιθυμούν να λάβουν μέρος στο διαγωνισμό πρέπει να καταθέσουν μέσω του νομίμου εκπροσώπου τους, ή εξουσιοδοτημένου αντιπροσώπου, ιδιοχείρως ή αποστέλλοντας ταχυδρομικά με συστημένη επιστολή ή μέσω courier στον ΔΣΑ, τις προσφορές τους, έως και την ημερομηνία και ώρα υποβολής των προσφορών. Οι προσφορές θα αφορούν, **επί ποινή αποκλεισμού,** στο σύνολο της προμήθειας. Οι προσφέροντες δεν δικαιούνται ουδεμία αποζημίωση για δαπάνες σχετικές με τη συμμετοχή τους. Προσφορά που υποβλήθηκε μετά την καθορισμένη ημερομηνία και ώρα, δεν θα λαμβάνεται υπόψη και θα επιστρέφεται στον ενδιαφερόμενο.

2.2 Οι προσφορές θα πρέπει να υποβάλλονται, **επί ποινή αποκλεισμού,** στην Ελληνική Γλώσσα, να είναι δακτυλογραφημένες και να μη φέρουν παράτυπες διορθώσεις, σβησίματα, διαγραφές, προσθήκες κ.λπ. Θα πρέπει να είναι με τα ίδια στοιχεία εκτυπωτικής μηχανής και μονογεγραμμένες από τον διαγωνιζόμενο. Αν υπάρχουν διορθώσεις, προσθήκες κ.λπ. πρέπει αυτές να μονογράφονται από τον συμμετέχοντα. Η δε αρμόδια επιτροπή κατά τον έλεγχο θα μονογράψει τις προσθήκες κλπ και γενικά θα επιβεβαιώσει ότι αυτές έγιναν πριν την αποσφράγιση της προσφοράς. Οι προσφορές πρέπει να έχουν συνεχή αρίθμηση και υπογραφή του νόμιμου εκπροσώπου του συμμετέχοντος σε κάθε φύλλο τους. Εναλλακτικές προσφορές δεν γίνονται δεκτές και απορρίπτονται ως απαράδεκτες.

2.3 Οι προσφορές πρέπει να υποβληθούν μέσα σε **ενιαίο σφραγισμένο φάκελο,** ο οποίος πρέπει απαραίτητα να φέρει την ΕΠΩΝΥΜΙΑ και τα ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ (διεύθυνση, αριθμός τηλεφώνου, φαξ, ηλεκτρονική διεύθυνση) του συμμετέχοντος και να γράφει ευκρινώς και τις παρακάτω ενδείξεις:

ΕΠΩΝΥΜΙΑ / ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΥΜΜΕΤΕΧΟΝΤΟΣ

ΦΑΚΕΛΟΣ ΠΡΟΣΦΟΡΑΣ ΓΙΑ ΤΟΝ ΠΡΟΧΕΙΡΟ ΔΙΑΓΩΝΙΣΜΟ:

«ΠΡΟΜΗΘΕΙΑ ΥΠΗΡΕΣΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΟΠΣ ΟΛΟΜΕΛΕΙΑΣ»

ΑΝΑΘΕΤΟΥΣΑ ΑΡΧΗ: ΔΙΚΗΓΟΡΙΚΟΣ ΣΥΛΛΟΓΟΣ ΑΘΗΝΩΝ

ΗΜΕΡΟΜΗΝΙΑ ΔΙΕΝΕΡΓΕΙΑΣ ΔΙΑΓΩΝΙΣΜΟΥ: 30/06/2026

«Να μην ανοιχθεί από την ταχυδρομική υπηρεσία ή τη γραμματεία»

Ο ΕΝΙΑΙΟΣ ΦΑΚΕΛΟΣ ΚΑΘΕ ΠΡΟΣΦΟΡΑΣ ΘΑ ΠΡΕΠΕΙ ΝΑ ΠΕΡΙΛΑΜΒΑΝΕΙ:

Δύο (2) ξεχωριστούς σφραγισμένους επιμέρους φακέλους («Υποφακέλους»), ήτοι:

2.3.1 Φάκελος **«ΔΙΚΑΙΟΛΟΓΗΤΙΚΑ-ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ»:** στον οποίο θα περιλαμβάνονται τα τυπικά και λοιπά δικαιολογητικά που υποβάλλει υποχρεωτικά και **επί ποινή αποκλεισμού** ο προσφέρων καθώς και την τεχνική προσφορά του.

Τα δικαιολογητικά αυτά είναι:

α) Τα νομιμοποιητικά έγγραφα κάθε συμμετέχοντος, όπως επικυρωμένο αντίγραφο του ισχύοντος καταστατικού και τα ΦΕΚ στα οποία έχουν δημοσιευθεί το καταστατικό ίδρυσης και οι τροποποιήσεις του (για ΑΕ και ΕΠΕ),

επικυρωμένα αντίγραφα του καταστατικού και των τροποποιήσεών του (για ΟΕ και ΕΕ), στοιχεία και έγγραφα (πρωτότυπα ή επικυρωμένα αντίγραφα), από τα οποία πρέπει να προκύπτουν ο Πρόεδρος και Διευθύνων Σύμβουλος ΑΕ, τα υπόλοιπα πρόσωπα που έχουν δικαίωμα να δεσμεύουν με την υπογραφή τους το νομικό πρόσωπο και τα έγγραφα της νομιμοποίησης αυτών, αν αυτό δεν προκύπτει ευθέως από το καταστατικό αναλόγως με τη νομική μορφή των εταιρειών ή κάθε άλλου νομικού προσώπου.

β) Υπεύθυνη δήλωση του Ν. 1599/1986 (ΦΕΚ 75Α) του συμμετέχοντος στην οποία θα δηλώνεται ότι:

- Αποδέχεται ανεπιφύλακτα τους όρους της παρούσας διακήρυξης.
- Η προσφορά συντάχθηκε σύμφωνα με τους όρους της παρούσας διακήρυξης, των οποίων έλαβε πλήρη και ανεπιφύλακτη γνώση.
- Η υποβαλλόμενη προσφορά καλύπτει το σύνολο του υπό προμήθεια είδους.
- Τα στοιχεία που αναφέρονται στην προσφορά είναι αληθή και ακριβή.
- Παραιτείται από κάθε δικαίωμα αποζημίωσής του σχετικό με οποιαδήποτε απόφαση του ΔΣΑ για αναβολή ή ακύρωση του διαγωνισμού.
- Σε περίπτωση κατακύρωσης θα προσκομίσει στον ΔΣΑ τα πιστοποιητικά που αναφέρονται στον όρο 6 της παρούσης διακήρυξης.

γ) Υπεύθυνη δήλωση του Ν. 1599/1986 (ΦΕΚ 75Α), του συμμετέχοντος, σχετικά με τα αναφερόμενα στους όρους 1.2.1, 1.2.2., 1.2.3. 1.2.4 και 1.2.5 της παρούσας. Για τη συνδρομή των προϋποθέσεων του όρου 1.2.3. θα υποβάλλεται η ως άνω υπεύθυνη δήλωση, από κάθε πρόσωπο που αναφέρεται στον όρο αυτό.

<u>δ) Τα δικαιολογητικά με ποινή αποκλεισμού,απόδειξης τεχνικής και επαγγελματικής ικανότητας του συμμετέχοντα ήτοι:</u>

- Πίνακα Συναφών Έργων που έχουν εκτελεσθεί κατά την προηγούμενη τριετία, τα οποία αφορούν σε παρόμοια έργα και στον οποίο να αναγράφονται το αντικείμενο του έργου, η αναθέτουσα αρχή, ο προϋπολογισμός του έργου και η διάρκεια εκτέλεσης αυτού.

- Πιστοποιητικά ISO, όπως αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Β -Τεχνικές Προδιαγραφές – Παραδοτέα . Τα εν λόγω πιστοποιητικά θα περιλαμβάνονται στην τεχνική προσφορά του Αναδόχου σε έντυπη μορφή.
- Κατάλογο στον οποίο να αναφέρονται τα ονοματεπώνυμα των ατόμων που αποτελούν την ομάδα έργου του συμμετέχοντος..
- Σύντομα βιογραφικά σημειώματα στελεχών προτεινόμενης Ομάδας Έργου, τα οποία θα πρέπει να διαθέτουν εξειδικευμένη γνώση και εμπειρία για την εκτέλεση παρόμοιων έργων/ υπηρεσιών.

- Η Ομάδα Έργου θα απαρτίζεται από Έναν (1) Υπεύθυνο έργου ο οποίος θα πρέπει να είναι εργαζόμενος του υποψηφίου αναδόχου, να διαθέτει πτυχίο Πανεπιστημιακής Εκπαίδευσης, και να διαθέτει πιστοποιήσεις CISM, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 27701 Lead Auditor, ISO 27799 Senior Lead Manager.
- Έναν (1) Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών, ο οποίος θα πρέπει να είναι εργαζόμενος του υποψηφίου αναδόχου, να διαθέτει πτυχίο Πανεπιστημιακής Εκπαίδευσης, μεταπτυχιακό τίτλο σπουδών σε θέματα ασφάλειας πληροφοριών και να είναι πιστοποιημένος ISO 27001 Lead Auditor, ISO 27701 Lead Auditor, ISO 27799 Foundation, ISO 22301 Lead Auditor και CISA.
- Έναν (1) Σύμβουλος Κυβερνοασφάλειας, ο οποίος θα πρέπει να είναι εργαζόμενος του υποψηφίου αναδόχου να διαθέτει πτυχίο Πανεπιστημιακής Εκπαίδευσης, και να είναι πιστοποιημένος ISO 27032 Cybersecurity Manager, ISO 27799 Foundation και ISO 22301 Lead Auditor.
- Έναν (1) Νομικό Σύμβουλο, με επιστημονική εξειδίκευση και εμπειρία και στην υλοποίηση έργων ασφάλειας πληροφοριών και προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Νομικός Σύμβουλος θα πρέπει να είναι εργαζόμενος του αναδόχου και να έχει εμπειρία σε τουλάχιστον 3 έργα, τα τελευταία 2 έτη, στην υλοποίηση έργων ασφάλειας πληροφοριών.

Σε περίπτωση Ένωσης/Κοινοπραξίας τα δικαιολογητικά της παραγράφου αυτής (Άδεια παροχής λογιστικών και φοροτεχνικών υπηρεσιών, πιστοποιητικό ISO) αρκεί να αφορούν ένα από τα μέλη και να προσκομίζονται με την προσφορά.

ε) Δικαιολογητικά με ποινή αποκλεισμού, **απόδειξης οικονομικής και χρηματοοικονομικής επάρκειας του συμμετέχοντος:**

Δημοσιευμένοι ισολογισμοί ή αποσπάσματα ισολογισμών των τριών τελευταίων οικονομικών χρήσεων από τους οποίους πρέπει να προκύπτει ότι έχει μέσο ετήσιο κύκλο εργασιών άνω των τριακοσίων χιλιάδων (300.000,00) ευρώ.

Σε περίπτωση συμμετέχοντος που δεν έχει κατά νόμο υποχρέωση δημοσίευσης ισολογισμών, είναι υποχρεωτική η κατάθεση Υπεύθυνης Δήλωσης **θεωρημένης για το γνήσιο της υπογραφής της από αρμόδια αρχή,** περί της χρηματοοικονομικής του κατάστασης, κατά τα ανωτέρω, ή οποιουδήποτε άλλου σχετικού εγγράφου (φορολογικές δηλώσεις κλπ).

στ) Έγγραφο εκπροσώπησης, εφ' όσον ο συμμετέχων λαμβάνει μέρος στον διαγωνισμό με εκπρόσωπό του.

2.3.2. Σε περίπτωση υποβολής κοινής προσφοράς από Ένωση/Κοινοπραξία, όλα τα ανωτέρω δικαιολογητικά πρέπει να υποβάλλονται για κάθε μέλος. Επίσης πρέπει να υποβληθεί και το ισχύον συμφωνητικό σύστασης της Ένωσης/Κοινοπραξίας.

2.3.3. Την Τεχνική προσφορά Στον ως άνω φάκελο των δικαιολογητικών θα υπάρχει και η **Τεχνική προσφορά,** η οποία πρέπει επί ποινή αποκλεισμού να είναι σύμφωνη με το Παράρτημα Β της παρούσας και στην οποία θα δηλώνεται ρητά επί ποινή αποκλεισμού ότι γίνονται αποδεκτά τα αναγραφόμενα στο παράρτημα Β της παρούσης. Η τεχνική προσφορά θα είναι υπογεγραμμένη από τον υποψήφιο ανάδοχο.

2.3.4. Φάκελος **«ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ»**: ο οποίος θα πρέπει να περιέχει επί ποινή αποκλεισμού το Παράρτημα Γ της παρούσας, συμπληρωμένο με ευκρίνεια.

Στην οικονομική του προσφορά ο συμμετέχων θα πρέπει να αναφέρει τον χρόνο της ισχύος

της προσφοράς του, που θα είναι σύμφωνος με όσα αναφέρονται στην παρούσα διακήρυξη.

Σε περίπτωση που η προσφορά του συμμετέχοντος έχει χρονική διάρκεια μικρότερη της ζητούμενης από την διακήρυξη, η προσφορά απορρίπτεται ως απαράδεκτη.

Οι τιμές των προσφορών δεν υπόκεινται σε μεταβολή κατά τη διάρκεια ισχύος της προσφοράς, ούτε σε περίπτωση που ζητηθεί παράταση της διάρκειας ισχύος της προσφοράς.

Όλες οι τιμές θα είναι εκφρασμένες σε ευρώ και θα αναγράφονται αριθμητικά και ολογράφως. Σε περίπτωση που υπάρχει διαφορά μεταξύ των δύο αναγραφών, υπερισχύει η τιμή που έχει αναγραφεί ολογράφως. Προσφορές στις οποίες δεν προκύπτει με σαφήνεια η προσφερόμενη τιμή, απορρίπτονται. Η τιμή θα επιβαρύνεται μόνο με τον αναλογούντα φόρο προστιθέμενης αξίας (ΦΠΑ) ο οποίος θα βαρύνει τον ΔΣΑ.

Επίσης προσφορές που θέτουν όρο αναπροσαρμογής κατά την διάρκεια εκτέλεσης της σύμβασης απορρίπτονται ως απαράδεκτες.

Η προσφορά πρέπει να είναι υπογεγραμμένη σε κάθε φύλλο της και σε περίπτωση υποβολής κοινής προσφοράς από Ένωση/Κοινοπραξία από όλα τα μέλη της Ένωσης/Κοινοπραξίας.

3. Αξιολόγηση προσφορών

3.1 Κριτήριο ανάθεσης

Η αξιολόγηση της προμήθειας θα γίνει με κριτήριο κατακύρωσης τη πλέον συμφέρουσα από οικονομική άποψη προσφορά.

3.2 Κριτήρια τεχνικής αξιολόγησης

α/α	Κριτήριο Αξιολόγησης	Συντελεστής Βαρύτητας
1	Πληρότητα και λειτουργικότητα υπηρεσιών SOCaaS / MDR	30%

α/α	Κριτήριο Αξιολόγησης	Συντελεστής Βαρύτητας
2	SLA, χρόνοι απόκρισης και διαδικασίες διαχείρισης περιστατικών	20%
3	Μεθοδολογία υλοποίησης και επιχειρησιακής λειτουργίας	15%
4	Εμπειρία, επάρκεια και πιστοποιήσεις ομάδας έργου	15%
5	Δυνατότητες reporting, KPIs και continuous improvement	10%
6	Υπηρεσίες Penetration Testing και Vulnerability Management	10%

Το άθροισμα των συντελεστών βαρύτητας ισούται με 100%.

3.3 Βαθμολόγηση των Τεχνικών Προσφορών

Όλα τα επί μέρους κριτήρια βαθμολογούνται αυτόνομα με βάση τους εκατό (100) βαθμούς.

Η βαθμολογία των επί μέρους κριτηρίων των προσφορών είναι 100 βαθμοί για τις περιπτώσεις κατά τις οποίες καλύπτονται ακριβώς οι απαιτήσεις της διακήρυξης.

Η βαθμολογία αυτή αυξάνεται έως 110 βαθμούς στις περιπτώσεις κατά τις οποίες υπερκαλύπτονται οι απαιτήσεις της διακήρυξης και προσφέρονται πρόσθετες δυνατότητες ή πλεονεκτήματα τα οποία κρίνονται ουσιώδη για το έργο.

Η σταθμισμένη βαθμολογία κάθε επιμέρους κριτηρίου προκύπτει από το γινόμενο:

$Bi = Ki \times \Sigma i$

όπου:

- Bi = σταθμισμένη βαθμολογία κριτηρίου
- Ki = βαθμολογία επιμέρους κριτηρίου
- Σi = συντελεστής βαρύτητας κριτηρίου

Η συνολική βαθμολογία της τεχνικής προσφοράς προκύπτει από το άθροισμα των σταθμισμένων βαθμολογιών όλων των επιμέρους κριτηρίων.

3.4 Οικονομική Αξιολόγηση

Η οικονομική αξιολόγηση θα πραγματοποιηθεί με βάση τη συνολική οικονομική προσφορά του υποψηφίου αναδόχου για το σύνολο του έργου.

Ως συγκριτική τιμή λαμβάνεται η συνολική τιμή προσφοράς χωρίς ΦΠΑ.

3.5 Τελική Κατάταξη Προσφορών

Η κατακύρωση θα γίνει με κριτήριο τη συμφερότερη προσφορά.

Συμφερότερη θεωρείται η προσφορά που παρουσιάζει τον μικρότερο λόγο της συγκριτικής τιμής προσφοράς προς τη συνολική βαθμολογία της τεχνικής προσφοράς.

Ο λόγος αυτός υπολογίζεται σύμφωνα με τον ακόλουθο τύπο:

Λ = Τ / Β όπου:

- Λ = συγκριτικός λόγος προσφοράς
- Τ = συνολική οικονομική προσφορά χωρίς ΦΠΑ
- Β = συνολική βαθμολογία τεχνικής προσφοράς

Η προσφορά με το μικρότερο Λ κατατάσσεται πρώτη.

4. Ισχύς προσφορών

Οι προσφορές ισχύουν και δεσμεύουν τους συμμετέχοντες για ενενήντα (90) ημερολογιακές ημέρες από την επομένη της διενέργειας του διαγωνισμού.

Προσφορά που ορίζει μικρότερο χρόνο ισχύος ή δεν ορίζει καθόλου χρόνο ισχύος, απορρίπτεται ως απαράδεκτη.

Εάν προκύψει θέμα παράτασης της ισχύος των προσφορών ο ΔΣΑ θα απευθύνει έγγραφο ερώτημα προς τους συμμετέχοντες, πέντε (5) ημέρες πριν από τη λήξη ισχύος των προσφορών, αναφορικά με την αποδοχή παράτασης για συγκεκριμένο χρονικό διάστημα.

Οι συμμετέχοντες οφείλουν να απαντήσουν σχετικά μέσα σε τρεις (3) ημέρες.

Η ανακοίνωση της κατακύρωσης του Διαγωνισμού στον ανάδοχο μπορεί να γίνεται

και μετά τη λήξη της ισχύος της προσφοράς, τον δεσμεύει όμως μόνο εφόσον αυτός το αποδεχθεί.

5. Διάρκεια Σύμβασης

Η διάρκεια της σύμβασης ορίζεται σε ένα **(1) έτος**, από την υπογραφή της, με δυνατότητα ισόχρονης ανανέωσης.

6. Επιλογή Αναδόχου – Κατακύρωση διαγωνισμού

6.1 Η επιλογή Αναδόχου και η κατακύρωση των αποτελεσμάτων του διαγωνισμού θα γίνει στον συμμετέχοντα- που πληροί τους όρους της διακήρυξης ως προς τα δικαιολογητικά και η τεχνική του προσφορά έγινε αποδεκτή- και ο οποίος προσέφερε την πλέον συμφέρουσα από οικονομική άποψη προσφορά για το σύνολο του έργου, με απόφαση του αρμοδίου οργάνου του ΔΣΑ, μετά από σχετική εισήγηση της επιτροπής του διαγωνισμού.

6.2 Μετά την αξιολόγηση των προσφορών, ο συμμετέχων στον οποίο πρόκειται να γίνει η κατακύρωση οφείλει, εντός προθεσμίας δέκα (10) ημερών από την κοινοποίηση σ' αυτόν της σχετικής έγγραφης ειδοποίησης του ΔΣΑ, να υποβάλει στην Επιτροπή Διαγωνισμού, σε σφραγισμένο φάκελο, τα εξής έγγραφα και δικαιολογητικά από τις κατά περίπτωση αρμόδιες δικαστικές και διοικητικές αρχές, τα οποία αποσφραγίζονται και ελέγχονται από αυτήν:

α) Απόσπασμα ποινικού μητρώου έκδοσης του τελευταίου τριμήνου πριν από την κοινοποίηση της ως άνω έγγραφης ειδοποίησης, από το οποίο να προκύπτει, ότι τα πρόσωπα που ορίζονται στον όρο 1.1 δεν έχουν καταδικαστεί για τα αδικήματα που αναφέρονται στον όρο 1.2.3. της παρούσας, με αμετάκλητη απόφαση.

β) Πιστοποιητικό αρμόδιας δικαστικής ή διοικητικής αρχής έκδοσης του τελευταίου τριμήνου, πριν από την κοινοποίηση της ως άνω έγγραφης ειδοποίησης, από το οποίο να προκύπτει ότι δεν τελεί στις καταστάσεις που αναφέρονται στους όρους 1.2.1 και 1.2.4. της παρούσας.

γ) Πιστοποιητικό που εκδίδεται από αρμόδια κατά περίπτωση αρχή, από το οποίο να προκύπτει ότι κατά την προσκόμισή του είναι ενήμερος ως προς τις υποχρεώσεις του που αφορούν τις εισφορές κοινωνικής ασφάλισης (κύριας και επικουρικής) καθώς και ως προς τις φορολογικές υποχρεώσεις του.

δ) Υπεύθυνη δήλωση περί μη αποκλεισμού από δημόσιους διαγωνισμούς.

6.3 Εάν περάσει άπρακτη η παραπάνω προθεσμία χωρίς ο Ανάδοχος να αποστείλει τα απαιτούμενα δικαιολογητικά, για την υπογραφή της σύμβασης, ο ΔΣΑ μπορεί να τον κηρύξει έκπτωτο και να αποφασίσει την ανάθεση της προμήθειας στον επόμενο κατά σειρά κατάταξης.

6.4 Ο ΔΣΑ δεν δεσμεύεται για την τελική ανάθεση της σύμβασης και δικαιούται να την αναθέσει ή όχι, να ματαιώσει, να αναβάλει ή να επαναλάβει τη σχετική διαδικασία, χωρίς ουδεμία υποχρέωση για καταβολή αμοιβής ή αποζημίωσης εξ αυτού του λόγου στους συμμετέχοντες.

7. Κατάρτιση και υπογραφή της Σύμβασης – Εγγυητική Επιστολή Καλής Εκτέλεσης.

7.1 Μεταξύ του ΔΣΑ και του Αναδόχου στον οποίο κατακυρώθηκε το έργο υπογράφεται σύμβαση, σύμφωνα με τους όρους της παρούσας. Τυχόν υποβολή σχεδίων σύμβασης από τους συμμετέχοντες μαζί με τις προσφορές τους δεν δημιουργεί καμία δέσμευση για τον ΔΣΑ.

Η σύμβαση καταρτίζεται στην ελληνική γλώσσα με βάση τους όρους που περιλαμβάνονται στην διακήρυξη και την προσφορά του Αναδόχου όπως έγινε αποδεκτή κατά την κατακύρωση.

Το κείμενο της σύμβασης κατισχύει κάθε άλλου κειμένου στο οποίο στηρίζεται, εκτός κατάδηλων σφαλμάτων ή παραδρομών. Για θέματα που δεν ρυθμίζονται ρητά από τη σύμβαση και τα παραρτήματα αυτής ή σε περίπτωση που ανακύψουν αντικρουόμενοι/ αντιφατικοί όροι αυτής, για την ερμηνεία της

λαμβάνονται υπόψη κατά σειρά η παρούσα Διακήρυξη, η απόφαση κατακύρωσης και η προσφορά του Αναδόχου.

7.2 Ο Ανάδοχος στον οποίο κατακυρώθηκε η προμήθεια, υποχρεούται, να καταθέσει εγγυητική επιστολή καλής εκτέλεσης, κατά την υπογραφή της σχετικής σύμβασης, για την τήρηση των όρων της σύμβασης. Σε διαφορετική περίπτωση, κηρύσσεται έκπτωτος, και ο ΔΣΑ μπορεί να αποφασίσει την ανάθεση της προμήθειας στον επόμενο κατά σειρά κατάταξης.

Η Εγγυητική Επιστολή θα πρέπει να έχει εκδοθεί από αναγνωρισμένο πιστωτικό ίδρυμα ή άλλο νομικό πρόσωπο, που λειτουργούν νόμιμα στα κράτη μέλη της Ε.Ε. και έχουν σύμφωνα με τη νομοθεσία των κρατών μελών αυτό το δικαίωμα, ποσού ίσου με το 5% της οικονομικής προσφοράς του συμπεριλαμβανομένου του αναλογούντος Φ.Π.Α. Η εγγυητική επιστολή πρέπει να κατατεθεί προ ή έως την υπογραφή της σύμβασης.

Η εγγυητική επιστολή πρέπει να έχει διάρκεια ισχύος ένα (1) μήνα μετά την ημερομηνία παράδοσης του είδους. Εάν η εγγυητική επιστολή εκδοθεί από μη ελληνική Τράπεζα, τότε μπορεί να είναι συντεταγμένη σε μία από τις επίσημες γλώσσες της Ευρωπαϊκής Κοινότητας, αλλά θα συνοδεύεται απαραίτητα από επίσημη επικυρωμένη μετάφραση στην ελληνική γλώσσα, η οποία υπερισχύει της ξενόγλωσσης διατύπωσης.

Σε περίπτωση Ένωσης /Κοινοπραξίας θα πρέπει να σημειώνεται στην εγγύηση καλής εκτέλεσης ότι αυτή καλύπτει όλα τα μέλη της ένωσης /κοινοπραξίας, αλληλεγγύως. Η εγγυητική επιστολή καλής εκτέλεσης επιστρέφεται στον Ανάδοχο μετά την οριστική παραλαβή του υπό προμήθεια είδους, σύμφωνα με τα οριζόμενα στη σύμβαση. Εναλλακτικώς, η παραπάνω εγγύηση για την καλή εκτέλεση δύναται να δοθεί και με καταβολή του αντίστοιχου ποσού στο ταμείο του ΔΣΑ, εκδιδομένου προς τούτο αντίστοιχου αποδεικτικού καταβολής, στο οποίο θα αναγράφονται τα στοιχεία της σύμβασης στην οποία αφορά, σύμφωνα με το άρθρο 31 παρ.1 του Κανονισμού Προμηθειών του ΔΣΑ. Για την ως άνω εγγύηση ισχύουν αναλόγως οι προβλέψεις της προηγούμενης παραγράφου για την εγγυητική επιστολή καλής εκτέλεσης.

7.3. Οι τιμές των προσφορών δεν υπόκεινται σε οποιαδήποτε αναπροσαρμογή κατά τη διάρκεια ισχύος της σύμβασης. Ο ΔΣΑ διατηρεί το δικαίωμα να ζητήσει από τους συμμετέχοντες στοιχεία απαραίτητα για την τεκμηρίωση της προσφερόμενης τιμής.

8. Παραλαβή

Η παραλαβή του υπό προμήθεια είδους θα γίνει στα γραφεία του ΔΣΑ (Ακαδημίας 60 –Αθήνα) από την επιτροπή παραλαβής που θα υποδείξει εγγράφως ο ΔΣΑ στον ανάδοχο.

9. Τρόπος πληρωμής του Αναδόχου

Η συμφωνηθείσα αμοιβή του Αναδόχου θα καταβληθεί εντός είκοσι (20) ημερών από την οριστική ποσοτική και ποιοτική παραλαβή των τευχών από τον ΔΣΑ, με την έκδοση του πρωτοκόλλου παραλαβής και του τιμολογίου από τον Ανάδοχο. Ο Ανάδοχος προκειμένου να εισπράξει την αμοιβή του υποχρεούται στην προσκόμιση των νόμιμων παραστατικών και δικαιολογητικών που προβλέπονται από τις ισχύουσες διατάξεις καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

10. Τρόπος λήψης εγγράφων διαγωνισμού- Πληροφορίες

Οι ενδιαφερόμενοι μπορούν να παραλαμβάνουν τη Διακήρυξη από τα γραφεία του ΔΣΑ (οδός Ακαδημίας αρ. 60, ΤΚ 10679, Αθήνα), μετά από την υποβολή σχετικής αίτησης στην οποία θα αναγράφονται τα στοιχεία επικοινωνίας τους (επωνυμία, διεύθυνση, τηλέφωνο, φαξ, e-mail).

Οι παραλήπτες της Διακήρυξης υποχρεούνται να ελέγξουν άμεσα το αντίτυπο που παραλαμβάνουν και εφόσον διαπιστώσουν οποιαδήποτε παράλειψη να το γνωρίσουν εγγράφως στον ΔΣΑ προκειμένου να λάβουν νέο πλήρες αντίγραφο. Οι ενδιαφερόμενοι μπορούν να ζητήσουν εγγράφως (με επιστολή ή τηλεομοιοτυπία απευθυνόμενη προς τον ΔΣΑ, συμπληρωματικές πληροφορίες ή διευκρινίσεις σχετικά με τους όρους της διακήρυξης.

Κανένας υποψήφιος δεν μπορεί σε οποιαδήποτε περίπτωση να επικαλεσθεί προφορικές απαντήσεις εκ μέρους οποιουδήποτε υπαλλήλου του ΔΣΑ σχετικά με τους όρους του Διαγωνισμού.

ΠΑΡΑΡΤΗΜΑ Β

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ- ΠΑΡΑΔΟΤΕΑ

Το παρόν έργο αφορά την προμήθεια υπηρεσιών Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (Security Operations Center - Managed Security Services, SOC MSS), με συνεχή λειτουργία 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα (24x7), για χρονικό διάστημα ένα (1) έτος με δυνατότητα ισόχρονης ανανέωσης..

Σκοπός του έργου είναι η παρακολούθηση, ανάλυση και αντιμετώπιση περιστατικών ασφάλειας με στόχο την ενίσχυση της κυβερνοασφάλειας και την προστασία των ψηφιακών υποδομών του ΟΠΣ Ολομέλειας ώστε να παρέχει ένα ολοκληρωμένο, πολυεπίπεδο και βασισμένο στην Τεχνητή Νοημοσύνη πλαίσιο άμυνας σε βάθος για την προστασία δεδομένων, εφαρμογών και υποδομών στο περιβάλλον του Gcloud – Azure

Ειδικότερα:

Αντικείμενο RFP

Ο Φορέας προτίθεται να αναθέσει υπηρεσίες **Security Operations Center as a Service (SOCaaS)** και **MDR (Managed Detection & Response)**, με στόχο τη συνεχή επιτήρηση της πληροφοριακής υποδομής, την έγκαιρη ανίχνευση και τεκμηριωμένη διερεύνηση συμβάντων ασφάλειας, καθώς και την υποστήριξη ενεργειών απόκρισης σε συνεργασία με τις αρμόδιες τεχνικές ομάδες.

Οι υπηρεσίες θα παρέχονται σε περιβάλλον παραγωγής, με ενεργά μέτρα προστασίας (ενδεικτικά firewalls, EDR, identity controls, cloud security controls) και απαιτούν ενοποιημένη δυνατότητα συλλογής, ανάλυσης, συσχέτισης και διαχείρισης περιστατικών, με πλήρη ιχνηλασιμότητα ενεργειών και μετρήσιμους δείκτες απόδοσης.

Η παροχή των υπηρεσιών θα έχει χρονική διάρκεια ίση με ένα **(1) έτος**, με δυνατότητα ισόχρονης ανανέωσης.

Επίσης, προτίθεται να αναθέσει υπηρεσίες **Τεχνικής Αξιολόγησης Ασφάλειας (Technical Security Assessments / Penetration Testing)** με στόχο την προληπτική αποτίμηση του επιπέδου ασφαλείας της υποδομής, των εφαρμογών και των ασύρματων δικτύων του.

Οι υπηρεσίες αφορούν ρεαλιστικές δοκιμές υπό κανονικές συνθήκες άμυνας, με ενεργά συστήματα ασφαλείας και παρακολούθηση από SOC, και περιλαμβάνουν επιβεβαίωση ευρημάτων μέσω ελεγχόμενου exploitation, όπου αυτό είναι ασφαλές και εξουσιοδοτημένο.

Οι συγκεκριμένες υπηρεσίες θα εκτελεστούν 1 φορά (εξαιρουμένου του re-test) κατά τη διάρκεια της σύμβασης.

Ζητούμενες Υπηρεσίες

Οι υποψήφιοι ανάδοχοι καλούνται να υποβάλουν τεχνική και οικονομική προσφορά για τις παρακάτω υπηρεσίες οι οποίες περιλαμβάνουν κατ’ ελάχιστον:

- **SOC as a Service with MDR**
    - Συλλογή, κανονικοποίηση και αξιοποίηση δεδομένων καταγραφής από καθορισμένες πηγές (assets/log sources),

- Συνεχή παρακολούθηση και ανίχνευση συμβάντων ασφάλειας,
- Απόκριση σε συμβάντα ασφαλείας μέσω αυτοματοποιημένων ροών ενεργειών (playbooks)
- Διερεύνηση και τεκμηριωμένη διαχείριση περιστατικών,
- Ειδοποίηση και κλιμάκωση βάσει προκαθορισμένων επιπέδων σοβαρότητας,
- Παραγωγή περιοδικών αναφορών και δεικτών απόδοσης (KPIs).
- Άδειες EDR για όλα τα υπό-παρακολούθηση συστήματα (όπου μπορεί να εφαρμοστεί)

- **Penetration Testing**
  - Web Application Penetration Testing (σε 3 διαφορετικά web apps).

Γενικές Τεχνικές Απαιτήσεις

Ο ανάδοχος οφείλει να παρέχει τις ζητούμενες υπηρεσίες **SOCaaS** και **MDR** με επιχειρησιακή ωριμότητα, τεκμηριωμένες διαδικασίες και δυνατότητα απόδειξης κάλυψης (coverage) ανά κατηγορία asset/log source. Η υπηρεσία θα πρέπει να βασίζεται σε ενιαίο λειτουργικό περιβάλλον για βασικές λειτουργίες συλλογής, ανάλυσης, διερεύνησης και διαχείρισης περιστατικών, χωρίς να απαιτείται χρήση πρόσθετων ανεξάρτητων συστημάτων για τη βασική επιχειρησιακή ροή.

Ειδικότερα, ο ανάδοχος οφείλει να τεκμηριώσει ότι:

- υποστηρίζεται συλλογή δεδομένων καταγραφής από ετερογενείς πηγές (endpoints/servers, identity, network/security controls, cloud services), με κανονικοποίηση/συσχέτιση και δυνατότητα αναζήτησης,
- η διερεύνηση περιστατικών υλοποιείται μέσω case/incident management με μοναδική ταυτοποίηση, χρονογραμμή ενεργειών και τεκμηριωμένο συμπέρασμα,
- υφίσταται δομημένο μοντέλο κλιμάκωσης (escalation) βάσει σοβαρότητας (severity) και ρόλων, με σαφή χρονικά όρια απόκρισης,
- υφίσταται δυνατότητα εμπλουτισμού (enrichment) με εσωτερικά/εξωτερικά συμφραζόμενα (π.χ. identity attributes, reputation, DNS/WHOIS) ώστε να μειώνεται ο χρόνος διερεύνησης,
- υφίσταται διαδικασία συνεχούς βελτιστοποίησης (continuous tuning) και διαχείρισης ψευδώς θετικών (false positives) με τεκμηρίωση αποφάσεων,
- υφίσταται δυνατότητα αυτοματοποίησης ενεργειών απόκρισης με ασφαλιστικές δικλείδες (approvals/safeguards) και ιχνηλασιμότητα.

Η υπηρεσία θα λειτουργεί σε περιβάλλον παραγωγής. Ως εκ τούτου, κάθε ενέργεια που δύναται να επηρεάσει τη διαθεσιμότητα ή τη λειτουργικότητα συστημάτων (π.χ. containment, account disablement, network blocks) θα υπόκειται σε καθορισμένους κανόνες έγκρισης/εξουσιοδότησης, βάσει συμφωνημένης πολιτικής και ρόλων του Φορέα.

Αναφορικά με τις υπηρεσίες **Penetration Testing**, ο ανάδοχος οφείλει να εκτελέσει τις ζητούμενες υπηρεσίες εφαρμόζοντας αναγνωρισμένες και τεκμηριωμένες μεθοδολογίες

penetration testing, με στόχο τη ρεαλιστική αποτύπωση της επιφάνειας επίθεσης και της πραγματικής ανθεκτικότητας των πληροφοριακών συστημάτων του Φορέα. Η προσέγγιση της αξιολόγησης θα ευθυγραμμίζεται με σενάρια πραγματικού επιτιθέμενου και όχι με θεωρητική ή εργαστηριακή προσομοίωση.

Κατά τη διάρκεια της εκτέλεσης των δοκιμών θα υπάρχει ενεργή παρακολούθηση από το Security Operations Center (SOC), με συντονισμό μεταξύ των εμπλεκόμενων ομάδων. Η παρακολούθηση αυτή αποσκοπεί τόσο στη διασφάλιση της ομαλής λειτουργίας των συστημάτων όσο και στην αποτίμηση της επιχειρησιακής ορατότητας και απόκρισης.

Στις υπηρεσίες αυτές περιλαμβάνονται και στοχευμένο re-test προς επαλήθευση των όποιων διορθωτικών ενεργειών του Φορέα.

Στο πλαίσιο του έργου:

- δεν θα πραγματοποιηθούν δοκιμές Denial-of-Service ή stress testing,
- η επιβεβαίωση ευρημάτων θα γίνεται μέσω ελεγχόμενου exploitation, αποκλειστικά όπου αυτό είναι ασφαλές, τεχνικά εφικτό και ρητά εξουσιοδοτημένο,
- σε περιβάλλοντα παραγωγής θα λαμβάνονται όλα τα απαραίτητα μέτρα για την αποφυγή διακοπής υπηρεσιών ή απώλειας δεδομένων.

Πλαίσιο Σοβαρότητας και SLA

Η παρεχόμενη υπηρεσία SOCaaS και MDR θα διέπεται από προκαθορισμένο πλαίσιο ταξινόμησης περιστατικών (severity classification framework), το οποίο θα περιλαμβάνει κατ' ελάχιστον τα ακόλουθα επίπεδα:

- Critical
- High
- Medium
- Low
- Informational

Ο Ανάδοχος οφείλει να προτείνει σαφώς τεκμηριωμένο SLA ανά επίπεδο σοβαρότητας, το οποίο θα περιλαμβάνει:

- Χρόνο αρχικής απόκρισης (initial response time),
- Χρόνο έναρξης διερεύνησης (investigation start),
- Συχνότητα ενημέρωσης του Φορέα για ανοιχτά περιστατικά,
- Στόχο χρόνου ολοκλήρωσης διερεύνησης (όπου αυτό είναι εφαρμόσιμο).

Τα SLA θα πρέπει να μετρώνται με αντικειμενικό και επαναλήψιμο τρόπο, βάσει χρονοσήμανσης ενεργειών εντός του συστήματος διαχείρισης περιστατικών.

Η μεθοδολογία υπολογισμού βασικών δεικτών απόδοσης (όπως MTTD και MTTR) θα πρέπει να περιγράφεται σαφώς στην τεχνική προσφορά, ώστε να διασφαλίζεται διαφάνεια και συγκρισιμότητα.

Σε περιπτώσεις όπου η καθυστέρηση οφείλεται σε εξαρτήσεις από τον Φορέα (π.χ. αναμονή έγκρισης, πρόσβασης ή ενέργειας τρίτου), η περίοδος αυτή θα αποτυπώνεται διακριτά.

Ο Φορέας διατηρεί το δικαίωμα να ζητήσει από τον Ανάδοχο δείγμα μηνιαίας αναφοράς SLA και KPI πριν την ανάθεση.

Παραδοτέα

Αναφορικά με τις Υπηρεσίες **SOCaaS** και **MDR**, από την έναρξη λειτουργίας και καθ' όλη τη διάρκεια της σύμβασης, ο ανάδοχος υποχρεούται να παραδίδει πλήρες σύνολο παραδοτέων που να μπορεί να χρησιμοποιηθεί τόσο από τεχνικές ομάδες όσο και από τη διοίκηση του Φορέα, με σαφή αποτύπωση κινδύνου, τάσεων και απόδοσης υπηρεσίας.

Τα παραδοτέα θα περιλαμβάνουν κατ' ελάχιστον:

- Μηνιαίες περιοδικές αναφορές με KPIs/SLA (π.χ. MTTD, MTTR, κατανομή severity, τάσεις, κατηγορίες περιστατικών, συνοπτική αποτίμηση βελτιωτικών ενεργειών),
- Αναφορές περιστατικών (incident reports) με τεκμηριωμένο timeline, evidences, ενέργειες, συμπέρασμα και προτεινόμενες ενέργειες,
- Συνοπτική αναφορά συνεχούς βελτιστοποίησης (tuning report) με περιγραφή ουσιωδών αλλαγών/βελτιώσεων στην ανίχνευση και στη μείωση θορύβου,

Αναφορικά με τις υπηρεσίες **Penetration Testing**, ο ανάδοχος υποχρεούται να παραδώσει πλήρη και τεκμηριωμένη τεχνική αναφορά, η οποία θα μπορεί να χρησιμοποιηθεί τόσο από τεχνικές ομάδες όσο και από τη διοίκηση του Φορέα. Η αναφορά θα αποτυπώνει με σαφήνεια το επίπεδο κινδύνου, τα κρίσιμα ευρήματα και τις προτεραιότητες αντιμετώπισης.

Η τεχνική αναφορά θα περιλαμβάνει κατ' ελάχιστον:

- εκτελεστική σύνοψη (Executive Summary) με έμφαση στον επιχειρησιακό αντίκτυπο και τη συνολική στάθμη κινδύνου,
- περιγραφή της μεθοδολογίας και του πεδίου της αξιολόγησης,
- αναλυτική παρουσίαση όλων των ευρημάτων, με τεχνική ανάλυση και αποδεικτικά στοιχεία (evidence),
- αξιολόγηση σοβαρότητας και κινδύνου με βάση τεχνικά και επιχειρησιακά κριτήρια,
- σαφείς, εφαρμόσιμες και προτεραιοποιημένες προτάσεις remediation και hardening.

Δομή και Περιεχόμενο Τεχνικής Προσφοράς

Η προσφορά του υποψηφίου αναδόχου θα πρέπει να είναι σαφώς δομημένη, πλήρης και διατυπωμένη κατά τρόπο που να επιτρέπει αντικειμενική αξιολόγηση και συγκρισιμότητα μεταξύ των συμμετεχόντων και θα αφορά στο σύνολο των ζητούμενων υπηρεσιών.

Για τις υπηρεσίες **SOCaaS** και **MDR**, η τεχνική προσφορά θα περιλαμβάνει, κατ' ελάχιστον:

- συμπληρωμένο τον Πίνακα Τεχνικών Προδιαγραφών με σαφή δήλωση συμμόρφωσης ανά απαίτηση και τεκμηριωμένη απάντηση,

- περιγραφή του επιχειρησιακού μοντέλου παροχής υπηρεσίας (roles, διαδικασίες, τρόπος χειρισμού περιστατικών, escalation),
- περιγραφή του προτεινόμενου τρόπου υλοποίησης (onboarding approach, validation steps),
- ενδεικτικό χρονοδιάγραμμα υλοποίησης και μετάβασης σε steady-state λειτουργία.

Για τις υπηρεσίες **Penetration Testing**, η τεχνική προσφορά θα περιλαμβάνει, κατ' ελάχιστον:

- συμπληρωμένο τον Πίνακα Τεχνικών Προδιαγραφών με σαφή δήλωση συμμόρφωσης ανά απαίτηση,
- συνοπτική περιγραφή της προτεινόμενης μεθοδολογίας, των τεχνικών και των εργαλείων που θα χρησιμοποιηθούν, χωρίς αποκάλυψη ευαίσθητων λεπτομερειών,
- στοιχεία για την ομάδα έργου και την αποδεδειγμένη εμπειρία της σε αντίστοιχα έργα,
- ενδεικτικό χρονοδιάγραμμα υλοποίησης.

Απαιτήσεις Υποψηφίου Αναδόχου & Ομάδας Έργου

Αναφορικά με τις υπηρεσίες SOCaaS και MDR, ο υποψήφιος ανάδοχος οφείλει να διαθέτει ομάδα έργου που να περιλαμβάνει έμπειρα στελέχη που έχουν εμπλακεί σε ολοκληρωμένα ή υπό υλοποίηση έργα ασφάλειας πληροφοριών και τα οποία θα καλύπτουν κατ' ελάχιστο τις ακόλουθες κατηγορίες:

- Έναν (1) **Υπεύθυνο έργου** ο οποίος θα πρέπει να είναι **εργαζόμενος του υποψηφίου αναδόχου**, να διαθέτει **πτυχίο Πανεπιστημιακής Εκπαίδευσης**, και να διαθέτει πιστοποιήσεις **CISM, ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, ISO 27701 Lead Auditor, ISO 27799 Senior Lead Manager**.
- Έναν (1) **Υπεύθυνο Διαχείρισης Ασφάλειας Πληροφοριών,** ο οποίος θα πρέπει να είναι **εργαζόμενος του υποψηφίου αναδόχου,** να διαθέτει **πτυχίο Πανεπιστημιακής Εκπαίδευσης, μεταπτυχιακό τίτλο σπουδών σε θέματα ασφάλειας πληροφοριών** και να είναι πιστοποιημένος **ISO 27001 Lead Auditor, ISO 27701 Lead Auditor, ISO 27799 Foundation, ISO 22301 Lead Auditor και CISA.**
- Έναν (1) **Σύμβουλος Κυβερνοασφάλειας,** ο οποίος θα πρέπει να είναι **εργαζόμενος του υποψηφίου αναδόχου** να διαθέτει **πτυχίο Πανεπιστημιακής Εκπαίδευσης**, και να είναι πιστοποιημένος **ISO 27032 Cybersecurity Manager, ISO 27799 Foundation και ISO 22301 Lead Auditor**.
- Έναν (1) **Νομικό Σύμβουλο**, με επιστημονική εξειδίκευση και εμπειρία και στην υλοποίηση έργων ασφάλειας πληροφοριών και προστασίας δεδομένων προσωπικού χαρακτήρα. Ο Νομικός Σύμβουλος θα πρέπει να είναι εργαζόμενος του αναδόχου και να έχει εμπειρία σε τουλάχιστον 3 έργα, τα τελευταία 2 έτη, στην υλοποίηση έργων ασφάλειας πληροφοριών.

Αναφορικά με τις Υπηρεσίες **Penetration Testing**, ο υποψήφιος ανάδοχος οφείλει να διαθέτει ομάδα έργου (δεν αποκλείονται τυχόν υπεργολαβίες) με αποδεδειγμένη τεχνική επάρκεια και εμπειρία στην παροχή προηγμένων υπηρεσιών Penetration Testing και offensive security, πέραν βασικών ή αυτοματοποιημένων ελέγχων ευπαθειών. Η υλοποίηση του έργου θα πρέπει να πραγματοποιηθεί από εξειδικευμένη ομάδα, με εμπειρία σε σύνθετα περιβάλλοντα παραγωγής και ρεαλιστικά σενάρια απειλών.

Η ομάδα έργου θα πρέπει, σε συλλογικό επίπεδο, να καλύπτει τα βασικά τεχνικά αντικείμενα που σχετίζονται με το παρόν έργο, όπως ενδεικτικά:

- προηγμένο penetration testing υποδομών και λειτουργικών συστημάτων,
- web application και API security testing,
- τεχνικές post-exploitation, privilege escalation και lateral movement,
- offensive security και red teaming τεχνικές,
- κατανόηση σύγχρονων adversary techniques και threat intelligence.

Η τεχνική επάρκεια της ομάδας θα πρέπει να τεκμηριώνεται μέσω διεθνώς αναγνωρισμένων επαγγελματικών πιστοποιήσεων, οι οποίες να αντιστοιχούν στα ανωτέρω αντικείμενα. Οι πιστοποιήσεις αυτές δύνανται να κατανέμονται σε διαφορετικά μέλη της ομάδας έργου και δεν απαιτείται κάθε μέλος να κατέχει το σύνολο αυτών.

Επιπλέον, για έργα που εκτελούνται σε περιβάλλοντα αυξημένης ευαισθησίας ή με αυστηρές απαιτήσεις εμπιστευτικότητας, ο ανάδοχος θα πρέπει να δύναται να διαθέσει προσωπικό με ενεργή ή πρόσφατη διαπίστευση ασφάλειας (security clearance) σε εθνικό, ευρωπαϊκό ή διεθνές επίπεδο, εφόσον αυτό απαιτηθεί από τη φύση του έργου.

Ο Φορέας διατηρεί το δικαίωμα να ζητήσει τεκμηρίωση των ανωτέρω στοιχείων σε επίπεδο ομάδας έργου, χωρίς απαίτηση αποκάλυψης προσωπικών δεδομένων

Πρότυπα

Ο υποψήφιος Ανάδοχος απαιτείται να διαθέτει κατ' ελάχιστο τα ακόλουθα πιστοποιητικά τα οποία πρέπει να είναι σε ισχύ και να έχουν εκδοθεί από φορέα πιστοποίησης διαπιστευμένο από το ΕΣΥΔ ή από άλλο φορέα διαπίστευσης του εξωτερικού που διαθέτει αμοιβαία αναγνώριση από το ΕΣΥΔ:

- πιστοποιημένο και εν ισχύ Σύστημα Διαχείρισης Ποιότητας, σύμφωνα με το πρότυπο ISO **9001:2015** ή ισοδύναμο,
- πιστοποιημένο και εν ισχύ Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών κατά ISO/IEC **27001:2022** ή ισοδύναμο,
- πιστοποιημένο και εν ισχύ Σύστημα Διαχείρισης Επιχειρησιακής Συνέχειας κατά ISO **22301:2019** ή ισοδύναμο,
- πιστοποιημένο και εν ισχύ Σύστημα Διαχείρισης Υπηρεσιών της Τεχνολογίας Πληροφοριών κατά **ISO 20000-1:2018** ή ισοδύναμο,
- πιστοποιημένο και εν ισχύ Σύστημα Περιβαλλοντικής Διαχείρισης κατά **ISO 14001:2015** ή ισοδύναμο,
- πιστοποιημένο και εν ισχύ Σύστημα διαχείρισης της Υγείας και Ασφάλειας της Εργασίας κατά **ISO 45001:2018** ή ισοδύναμο
- πιστοποιημένο και εν ισχύ Σύστημα διαχείρισης Προσωπικών Δεδομένων (Ιδιωτικότητας) κατά **ISO/IEC 27701:2019** ή ισοδύναμο.
- πιστοποιημένο και εν ισχύ Σύστημα Ενεργειακής Διαχείρισης κατά **ISO 50001:2018** ή ισοδύναμο και πιστοποιημένο και εν ισχύ Σύστημα Διαχείρισης κατά της Δωροδοκίας κατά **ISO 37001:2016** ή ισοδύναμο.

Πίνακες Προδιαγραφών

Ακολουθούν οι Πίνακες Τεχνικών Προδιαγραφών, στους οποίους ο υποψήφιος ανάδοχος οφείλει να δηλώσει συμμόρφωση ανά απαίτηση, παρέχοντας τεκμηριωμένη απάντηση και παραπομπές.

Πίνακες Προδιαγραφών SOCaaS και MDR

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	**Γενικές Τεχνικές Προδιαγραφές**			
1.1	Η Αναθέτουσα Αρχή απαιτεί η προσφερόμενη λύση να βασίζεται σε ενιαίο λειτουργικό περιβάλλον για συλλογή, κανονικοποίηση, ανάλυση, διερεύνηση και διαχείριση περιστατικών ασφάλειας. Ειδικότερα: • Τα δεδομένα καταγραφής, οι ειδοποιήσεις (alerts) και οι υποθέσεις (cases) πρέπει να συσχετίζονται και να διαχειρίζονται εντός της ίδιας πλατφόρμας. • Οι ροές αυτοματοποίησης και απόκρισης να υλοποιούνται στο ίδιο περιβάλλον διαχείρισης περιστατικών. • Η διαχείριση υποθέσεων (assignment, αλλαγή κατάστασης, επισύναψη evidences, audit trail) να πραγματοποιείται χωρίς απαίτηση χρήσης ανεξάρτητου εξωτερικού εργαλείου. Να τεκμηριωθεί η ενιαία ιχνηλασιμότητα από το επίπεδο log έως το επίπεδο incident και ενεργειών απόκρισης.	ΝΑΙ		
1.2	Ο υποψήφιος πάροχος οφείλει να καλύψει τα παρακάτω τεχνολογικά assets (ενδεικτικό αρχικό εύρος), παρέχοντας συλλογή και αξιοποίηση δεδομένων καταγραφής, συσχέτιση, ανάλυση, εμπλουτισμό, χειρισμό περιστατικών και παραγωγή αναφορών. • 25x Linux Servers • 11x Windows Servers • 1x Azure Gateway with WAF • 1x Azure Entra ID	ΝΑΙ		
1.3	Ο υποψήφιος πάροχος οφείλει να τεκμηριώσει: • Διαθεσιμότητα της πλατφόρμας (availability target) και σχετικό μοντέλο ανθεκτικότητας (redundancy/failover). • Διαδικασίες αντιμετώπισης διακοπών (incident communications, degraded mode λειτουργίας, backfill/forwarding). • Μηχανισμό εξασφάλισης συνέχειας συλλογής/διατήρησης δεδομένων σε περίπτωση προσωρινής μη διαθεσιμότητας της κονσόλας ή επιμέρους συνιστωσών.	ΝΑΙ		
1.4	Ο υποψήφιος πάροχος οφείλει να τεκμηριώσει ότι υποστηρίζεται η εξαγωγή στοιχείων/αποδεικτικών (incidents, ενέργειες, συνημμένα, αναφορές, αποτελέσματα αναζητήσεων) για audit/forensics με σαφή χρονική σήμανση, τεκμηρίωση πηγής και πλήρη ιχνηλασιμότητα.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.5	Ο υποψήφιος πάροχος οφείλει να παραδώσει κατά τη φάση του onboarding, Coverage Matrix που να περιγράφει για κάθε ζητούμενο asset/log source: • Τρόπο συλλογής (agentless/API/syslog/collector/agent). • Επίπεδο κάλυψης (events covered, parsing/normalization status, supported fields). • Κρίσιμες παραδοχές/εξαρτήσεις (π.χ. required audit policy, required permissions, API limits). • Τυχόν “blind spots” ή εξαιρέσεις και προτεινόμενο remediation plan.	ΝΑΙ		
1.6	Να παραδοθούν ελεγμένοι και επαληθευμένοι onboarding οδηγοί για κάθε τύπο log source, ώστε να επιταχύνεται η υλοποίηση και να μειώνεται το troubleshooting.	ΝΑΙ		
1.7	Ζητείται πολυκάναλη ειδοποίηση για σημαντικά περιστατικά, που να περιλαμβάνει ταυτόχρονη ενεργοποίηση διαφορετικών διαύλων επικοινωνίας (π.χ., Email, τηλεφωνική κλήση).	ΝΑΙ		
1.8	Ο πάροχος πρέπει να διαθέτει σύστημα διαχείρισης περιστατικών με τις εξής δυνατότητες: • Αυτόματη δημιουργία υπόθεσης (case) από κάθε alert με μοναδικό αναγνωριστικό. • Εκχώρηση υπόθεσης σε αναλυτή (assignment) και παρακολούθηση status (Open, In Progress, Resolved). • Παρακολούθηση και τεκμηρίωση KPIs όπως MTTD, MTTR κ.α..	ΝΑΙ		
1.9	Να παρέχονται μηνιαίες περιοδικές αναφορές σε μορφή κατάλληλη για διοικητική αξιολόγηση, οι οποίες να περιλαμβάνουν KPIs (MTTD/MTTR), κατανομή σοβαρότητας, τάσεις, κατηγορίες περιστατικών, δείκτες συμμόρφωσης SLA και συνοπτική αποτίμηση βελτιωτικών ενεργειών.	ΝΑΙ		
1.10	Να περιγραφεί αναλυτικά το Escalation Matrix και πώς αυτό υλοποιείται εντός του συστήματος, με mapping severity → ρόλοι → ομάδες, αυτόματη δρομολόγηση, alerts και fallback escalation policies. Να αναφερθεί αν οι ενέργειες καταγράφονται (auditability).	ΝΑΙ		
1.11	Ο υποψήφιος πάροχος οφείλει να διαθέτει τεκμηριωμένη διαδικασία συνεχούς βελτιστοποίησης των detection μηχανισμών (rule tuning), η οποία να βασίζεται στην καταγραφή και αξιολόγηση ψευδώς θετικών περιστατικών (false positives). Η διαδικασία πρέπει να περιλαμβάνει: • Μηχανισμό χαρακτηρισμού περιστατικών ως false positive από τους αναλυτές. • Καταγραφή του σχετικού ιστορικού και των σχετικών αποφάσεων σε audit trail. • Feedback μηχανισμό που να ενεργοποιεί την τροποποίηση detection κανόνων ή exclusion policies. • Περιοδική ενημέρωση του πελάτη με συνοπτικές αναφορές tuning ενεργειών, με αιτιολόγηση και ανάλυση αντικτύπου.	ΝΑΙ		
1.12	Να υποστηρίζεται άμεση εφαρμογή εξαιρέσεων/καταστολής θορύβου για συγκεκριμένα κριτήρια (π.χ. χρήστης, διεύθυνση, σύστημα, εφαρμογή), με δυνατότητα προσωρινής ή μόνιμης εφαρμογής και δυνατότητα ανάκλησης, χωρίς να απαιτείται	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διακοπή λειτουργίας ή χρονοβόρες αλλαγές στη ρύθμιση της υπηρεσίας.			
1.13	Ζητείται η δυνατότητα πλοήγησης από alert ή incident σε normalized log και τελικά σε raw log χωρίς χρήση τρίτων εργαλείων.	ΝΑΙ		
1.14	Να υποστηρίζεται η πλήρης συσχέτιση κανόνων ανίχνευσης, περιστατικών και playbooks με MITRE ATT&CK tactics & techniques.	ΝΑΙ		
1.15	Να υποστηρίζεται διαδικασία προτεραιοποίησης περιστατικών που λαμβάνει υπόψη τη σοβαρότητα του alert, την κρισιμότητα των εμπλεκόμενων συστημάτων, τη φήμη σχετικών δεικτών και τη συχνότητα εμφάνισης, βάσει παραμετροποιήσιμων κανόνων.	ΝΑΙ		
1.16	Να αποδεικνύεται η ύπαρξη λεπτομερούς καταγραφής ενεργειών των αναλυτών ανά alert/case: assignment, status change, enrichment, escalation, closure. Οι ενέργειες να είναι χρονοσημασμένες, με user identification και να μην μπορούν να τροποποιηθούν.	ΝΑΙ		
2.	**Εξειδικευμένες Προδιαγραφές**			
2.1	Η προσφερόμενη λύση πρέπει να διατηρεί διαθέσιμα προς αναζήτηση τα δεδομένα καταγραφής για τουλάχιστον έξι (6) μήνες, ώστε να υποστηρίζεται διερεύνηση περιστατικών, έλεγχοι συμμόρφωσης και ψηφιακή διερεύνηση. Τα δεδομένα να παραμένουν πλήρως αναζητήσιμα (searchable) καθ' όλη τη διάρκεια του retention, χωρίς μεταφορά σε offline archive που απαιτεί επαναφορά.	ΝΑΙ		
2.2	Ο υποψήφιος πάροχος οφείλει να παρέχει συνεχή εικόνα της εξωτερικής επιφάνειας έκθεσης του Οργανισμού (δημόσια εκτεθειμένες υπηρεσίες/συστήματα), με δυνατότητα εντοπισμού νέων ή μη δηλωμένων εκτεθειμένων στοιχείων, και ανάδειξης βασικών κινδύνων (π.χ. εκτεθειμένες υπηρεσίες, εσφαλμένες ρυθμίσεις).	ΝΑΙ		
2.3	Να προσφερθεί υπηρεσία MDR για συνεχή παρακολούθηση, επιβεβαίωση συμβάντων, διερεύνηση, threat hunting και υποστήριξη απόκρισης, συμπεριλαμβανομένων των απαιτούμενων αδειών, για τα υπο-παρακολούθηση συστήματα (servers) με κοινή απεικόνιση και ενιαία ιχνηλασιμότητα με τα υπόλοιπα συστήματα.	ΝΑΙ		
2.4	Ο υποψήφιος πάροχος οφείλει να εξασφαλίζει τη λογική απομόνωση δεδομένων και λειτουργιών ανά οργανισμό/πελάτη. Επιπλέον, θα πρέπει να υποστήριζεται, εφόσον ζητηθεί μελλοντικά, η δυνατότητα παροχής αποκλειστικού περιβάλλοντος λειτουργίας στον Φορέα.	ΝΑΙ		
2.5	Ο υποψήφιος πάροχος οφείλει να τεκμηριώσει ότι το σύστημα διερεύνησης παρέχει, ανά incident/case, ενιαία εικόνα διερεύνησης με συγκεντρωμένα ευρήματα/συσχετίσεις/χρονογραμμή ενεργειών, δυνατότητα ανάλυσης ανά χρήστη/σύστημα/διεύθυνση και καταγραφή τεκμηριωμένου συμπεράσματος του αναλυτή με αναφορά στα σχετικά στοιχεία. Να υποστηρίζεται εξαγωγή συνοπτικού	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	πορίσματος και βασικών στοιχείων για audit/compliance.			
2.6	Ο υποψήφιος πάροχος οφείλει να τεκμηριώσει διαδικασία διαχείρισης και συντήρησης των μηχανισμών ανίχνευσης (κανόνες, αναλυτικές μέθοδοι, περιπτώσεις χρήσης), η οποία να περιλαμβάνει ιστορικό αλλαγών, έλεγχο πριν την εφαρμογή, δυνατότητα επαναφοράς σε προηγούμενη έκδοση και περιοδική ανασκόπηση αποτελεσματικότητας/κάλυψης.	ΝΑΙ		
2.7	Να υποστηρίζεται αυτόματος εμπλουτισμός των περιστατικών με πληροφορίες αξιολόγησης δεικτών (π.χ. κακόβουλη φήμη διευθύνσεων/τομέων, στοιχεία DNS/WHOIS, γεωγραφική πληροφορία), με ενσωμάτωση των αποτελεσμάτων στην εικόνα διερεύνησης.	ΝΑΙ		
2.8	Να τεκμηριωθεί ότι οι αυτοματοποιημένες ενέργειες απόκρισης μπορούν να διέπονται από διαδικασίες έγκρισης και ασφαλιστικές δικλείδες, ώστε να αποτρέπονται λανθασμένες ή μη εξουσιοδοτημένες ενέργειες. Πρέπει να καταγράφονται οι εγκρίσεις/απορρίψεις (με χρήστη και χρόνο) και να υπάρχει τεκμηριωμένος τρόπος αναίρεσης ή αντισταθμιστικής ενέργειας όπου είναι εφικτό.	ΝΑΙ		
2.9	Να τεκμηριωθεί δυνατότητα εκτέλεσης ενεργειών περιορισμού/αποκατάστασης σε πολλαπλά επίπεδα, ενδεικτικά: λογαριασμοί/ταυτότητες, τερματικά συστήματα και δικτυακοί/ασφαλιστικοί μηχανισμοί. Οι ενέργειες να εκτελούνται με τυποποιημένες ροές, να καταγράφονται πλήρως και να υπόκεινται σε έγκριση όπου απαιτείται.	ΝΑΙ		
2.10	Να υποστηρίζεται αμφίδρομη διασύνδεση με σύστημα ticketing/ITSM, ώστε να υπάρχει κοινή εικόνα για την εξέλιξη του περιστατικού, συγχρονισμός βασικών πεδίων (κατάσταση, προτεραιότητα, ανάθεση), καθώς και ανταλλαγή σχολίων και συνημμένων. Να τεκμηριωθούν κανόνες αποφυγής διπλοεγγραφών/ασυνεπειών και ορισμού “υπεύθυνης πηγής ενημέρωσης”.	ΝΑΙ		
2.11	Απαιτείται δυνατότητα αυτοματοποιημένης απόκρισης μέσω αυτοματοποιημένων ροών ενεργειών που: • Ενεργοποιούνται βάσει κανόνων ή manual trigger. • Περιλαμβάνουν ενέργειες όπως block IP, quarantine host, disable user. • Τεκμηριώνουν τις ενέργειες και υποστηρίζουν rollback.	ΝΑΙ		
2.12	Απαίτηση enrichment των alerts με user context από Active Directory ή LDAP: • OU, Group Membership, Title, Department, Last Login • Να εμφανίζονται τα enriched fields εντός του alert/case view • Να τεκμηριωθεί η διαδικασία enrichment και παραδείγματα.	ΝΑΙ		
2.13	Ο υποψήφιος πάροχος οφείλει να αξιοποιεί δημόσιες πηγές πληροφόρησης απειλών όπως (ενδεικτικά) τα AlienVault OTX, Abuse.ch, Anomali Limo, MISP κ.ά., με τους εξής όρους: • Διασύνδεση μέσω TAXII/STIX, API integration ή άλλου τυπικού πρωτοκόλλου. • Χρήση των feeds για enrichment Indicators (IP, Domain, URL, Hashes) σε νέα ή υφιστάμενα incidents.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Συμμετοχή των feeds στον detection μηχανισμό μέσω correlation rules ή playbooks.			
2.14	Απαιτείται η περιοδική (ανά τρίμηνο) διενέργεια internal και external vulnerability assessments, με τεκμηριωμένη μεθοδολογία, χρήση εργαλείων και συνοδευτική αναφορά με επαλήθευση ευρημάτων.	ΝΑΙ		

Πίνακες Προδιαγραφών Penetration Testing

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.	**Γενικές Τεχνικές Προδιαγραφές**			
1.1	Η κάθε αξιολόγηση θα υλοποιηθεί ως Threat-Led Penetration Test (TLPT), με σενάριο-καθοδηγούμενη προσομοίωση επιτιθέμενου και όχι ως απλή λίστα ευπαθειών.	ΝΑΙ		
1.2	Η κάθε δοκιμή θα βασίζεται σε προκαθορισμένα ρεαλιστικά attack scenarios που αντικατοπτρίζουν σύγχρονες τεχνικές απειλών.	ΝΑΙ		
1.3	Ο ανάδοχος θα τεκμηριώνει πλήρη αλυσίδα επίθεσης (attack chain), αποδεικνύοντας εφικτότητα και επιχειρησιακό αντίκτυπο.	ΝΑΙ		
1.4	Η επιβεβαίωση ευρημάτων θα γίνεται μέσω ελεγχόμενου exploitation, αποκλειστικά για την τεκμηρίωση attack path feasibility.	ΝΑΙ		
1.5	Η κάθε δοκιμή θα εκτελείται με μη διαταρακτικό τρόπο, χωρίς να επηρεάζεται η διαθεσιμότητα της πλατφόρμας.	ΝΑΙ		
1.6	Η κάθε αξιολόγηση θα πραγματοποιηθεί στο παραγωγικό περιβάλλον (G-Cloud), με αυξημένα μέτρα ασφάλειας.	ΝΑΙ		
1.7	Τα ευρήματα θα αξιολογούνται βάσει τεχνικής σοβαρότητας και επιχειρησιακού αντίκτυπου (material impact).	ΝΑΙ		
1.8	Κάθε επιβεβαιωμένο σενάριο θα συνοδεύεται από τεκμηριωμένα αποδεικτικά στοιχεία.	ΝΑΙ		
1.9	Η κάθε δοκιμή θα εφαρμόζει αρχή ελαχιστοποίησης δεδομένων και συμμόρφωσης με GDPR.	ΝΑΙ		
1.10	Η κάθε δοκιμή θα περιλαμβάνει όλες τις ενεργές εφαρμογές διαλειτουργικότητας του ΟΠΣ Ολομέλειας με τρίτα συστήματατ	ΝΑΙ		
2.	**Web Application Penetration Testing (Portal)**			

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.1	Ο ανάδοχος θα τεκμηριώσει εφικτές αλυσίδες επίθεσης (attack paths), συνδυάζοντας πολλαπλές αδυναμίες όπου είναι δυνατό.	ΝΑΙ		
2.2	Θα αξιολογηθούν πλήρως οι μηχανισμοί αυθεντικοποίησης και διαχείρισης συνεδρίας.	ΝΑΙ		
2.3	Θα ελεγχθεί η ορθή επιβολή authorization μεταξύ των ρόλων (User, User Impersonator, Super Admin, Bar Association Admin).	ΝΑΙ		
2.4	Θα αξιολογηθούν σενάρια privilege escalation εντός της εφαρμογής.	ΝΑΙ		
2.5	Θα διερευνηθούν σενάρια κατάχρησης επιχειρησιακής λογικής και κρίσιμων συναλλαγών.	ΝΑΙ		
2.6	Θα αξιολογηθεί η επιβολή authorization σε επίπεδο API (π.χ. BOLA/BFLA).	ΝΑΙ		
2.7	Θα εξεταστούν σενάρια κατάχρησης tokens, sessions και authentication artifacts.	ΝΑΙ		
2.8	Θα διερευνηθεί δυνατότητα κατάχρησης ευαίσθητων endpoints, συμπεριλαμβανομένων upload λειτουργιών.	ΝΑΙ		
2.9	Θα τεκμηριωθεί δυνατότητα συνδυασμού χαμηλής/μεσαίας σοβαρότητας αδυναμιών σε σενάρια υψηλού αντίκτυπου.	ΝΑΙ		
2.10	Η επιβεβαίωση attack path θα γίνεται χωρίς μαζική εξαγωγή δεδομένων ή μη αναστρέψιμες ενέργειες.	ΝΑΙ		
2.11	Ενέργειες αυξημένου ρίσκου θα απαιτούν ρητή συνεννόηση με τον Φορέα.	ΝΑΙ		
3.	**Web Application Penetration Testing (BackOffice)**			
3.1	Η δοκιμή θα βασίζεται σε threat-led και scenario-driven προσομοίωση επιτιθέμενου, εστιάζοντας σε εφικτές αλυσίδες επίθεσης.	ΝΑΙ		
3.2	Η επιβεβαίωση ευρημάτων θα πραγματοποιείται μέσω ελεγχόμενου exploitation, αποκλειστικά όπου είναι ασφαλές και εξουσιοδοτημένο.	ΝΑΙ		
3.3	Οι δοκιμές θα εκτελούνται με τρόπο μη διαταρακτικό, χωρίς να επηρεάζεται η διαθεσιμότητα της εφαρμογής ή η σταθερότητα του περιβάλλοντος UAT.	ΝΑΙ		
3.4	Δεν θα πραγματοποιηθούν δοκιμές Denial-of-Service (DoS) ή stress testing.	ΝΑΙ		
3.5	Δεν επιτρέπεται whitelisting IP ή απενεργοποίηση μηχανισμών ασφαλείας, εκτός αν συμφωνηθεί ρητά.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.6	Θα λαμβάνονται υπόψη υφιστάμενοι μηχανισμοί ασφαλείας (WAF/IDS/IPS/SOC monitoring) και θα τεκμηριώνεται η πρακτική τους επίδραση στην εφικτότητα επίθεσης.	ΝΑΙ		
3.7	Τα ευρήματα θα αξιολογούνται βάσει τεχνικής σοβαρότητας και επιχειρησιακού αντίκτυπου (material impact).	ΝΑΙ		
3.8	Κάθε εύρημα θα συνοδεύεται από επαρκή αποδεικτικά στοιχεία και βήματα αναπαραγωγής.	ΝΑΙ		
3.9	Η δοκιμή θα εφαρμόζει αρχές ελαχιστοποίησης δεδομένων και ασφαλούς χειρισμού ευαίσθητων πληροφοριών.	ΝΑΙ		
3.10	Θα παρέχεται στοχευμένο re-test για επιβεβαίωση remediation στα ευρήματα που συνέβαλαν στα attack paths.	ΝΑΙ		
3.11	Η τελική αναφορά θα περιλαμβάνει τεχνική ανάλυση, εκτίμηση επιχειρησιακού κινδύνου και σαφείς προτάσεις remediation.	ΝΑΙ		
3.12	Η αξιολόγηση θα καλύπτει διοικητική web εφαρμογή Backoffice με εκτιμώμενες ~200 λειτουργικές οθόνες / διεπαφές.	ΝΑΙ		
3.13	Θα περιλαμβάνεται πλήρης έλεγχος διοικητικής διεπαφής (~35 οθόνες/forms), συμπεριλαμβανομένων privilege escalation paths.	ΝΑΙ		
3.14	Ο ανάδοχος θα αποδεικνύει ικανότητα αξιολόγησης εφαρμογών βασισμένων σε .NET Framework 4.6 και ExtJS.	ΝΑΙ		
3.15	Θα αξιολογηθούν πλήρως οι μηχανισμοί αυθεντικοποίησης και διαχείρισης συνεδρίας, συμπεριλαμβανομένων session lifecycle controls.	ΝΑΙ		
3.16	Θα εξεταστούν σενάρια token replay, session fixation, token leakage και improper session invalidation.	ΝΑΙ		
3.17	Θα ελεγχθεί η ορθή επιβολή access control για τους ρόλους: Admin, LogisInfo, Mitros, EsPraxis, ProEsPraxis.	ΝΑΙ		
3.18	Θα αξιολογηθεί δυνατότητα παράκαμψης ορίων ρόλων (horizontal & vertical privilege escalation).	ΝΑΙ		
3.19	Θα διερευνηθούν σενάρια κατάχρησης επιχειρησιακής λογικής (workflow manipulation, approval bypass, forced state changes).	ΝΑΙ		
3.20	Θα αξιολογηθεί δυνατότητα κατάχρησης διοικητικών και κρίσιμων επιχειρησιακών λειτουργιών με ουσιαστικό αντίκτυπο.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.21	Θα αξιολογηθούν ~90 διαθέσιμα API methods/endpoints στο πλαίσιο του scope.	ΝΑΙ		
3.22	Θα αξιολογηθεί η επιβολή authorization σε επίπεδο API (BOLA/BFLA).	ΝΑΙ		
3.23	Θα διερευνηθούν σενάρια κατάχρησης API που οδηγούν σε μη εξουσιοδοτημένες ενέργειες ή έκθεση δεδομένων.	ΝΑΙ		
3.24	Θα τεκμηριωθεί συνδυασμός χαμηλής/μεσαίας σοβαρότητας αδυναμιών σε ρεαλιστικά attack paths υψηλού αντίκτυπου.	ΝΑΙ		
3.25	Θα αξιολογηθεί η δυνατότητα compromise λογαριασμών και εκμετάλλευσης αυθεντικοποιημένων ροών.	ΝΑΙ		
3.26	Θα διερευνηθούν διαδρομές έκθεσης ευαίσθητων δεδομένων (προσωπικών ή οικονομικών).	ΝΑΙ		
3.27	Δεν επιτρέπονται μη αναστρέψιμες αλλαγές, μαζική εξαγωγή δεδομένων ή disruptive ενέργειες.	ΝΑΙ		
3.28	Η εκμετάλλευση θα περιορίζεται στο απολύτως απαραίτητο για τεκμηρίωση εφικτότητας επίθεσης.	ΝΑΙ		
3.29	Θα τεκμηριώνονται blocks, rate limits και συμπεριφορά αμυντικών μηχανισμών κατά την εκτέλεση σεναρίων.	ΝΑΙ		
4.	**Web Application Penetration Testing (ERP)**			
4.1	Η δοκιμή θα βασίζεται σε scenario-driven προσομοίωση επιτιθέμενου, εστιάζοντας σε εφικτές αλυσίδες επίθεσης και material business impact.	ΝΑΙ		
4.2	Η επιβεβαίωση ευρημάτων θα πραγματοποιείται μέσω ελεγχόμενου exploitation, αποκλειστικά όπου είναι ασφαλές και εξουσιοδοτημένο.	ΝΑΙ		
4.3	Οι δοκιμές θα εκτελούνται με τρόπο μη διαταρακτικό, χωρίς να επηρεάζεται η διαθεσιμότητα ή η σταθερότητα του περιβάλλοντος UAT.	ΝΑΙ		
4.4	Δεν θα πραγματοποιηθούν δοκιμές Denial-of-Service (DoS) ή stress/performance testing.	ΝΑΙ		
4.5	Δεν επιτρέπεται whitelisting IP ή απενεργοποίηση μηχανισμών ασφαλείας εκτός ρητής έγκρισης.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.6	Θα τεκμηριώνεται η πρακτική επίδραση WAF/NAC/IDS/IPS/SOC monitoring στην επιτυχία attack paths.	ΝΑΙ		
4.7	Τα ευρήματα θα αξιολογούνται βάσει τεχνικής σοβαρότητας και επιχειρησιακού αντίκτυπου στο ERP περιβάλλον.	ΝΑΙ		
4.8	Κάθε εύρημα θα συνοδεύεται από επαρκή αποδεικτικά στοιχεία και βήματα αναπαραγωγής.	ΝΑΙ		
4.9	Η δοκιμή θα εφαρμόζει αρχές ελαχιστοποίησης δεδομένων και ασφαλούς χειρισμού προσωπικών, μισθολογικών και λογιστικών πληροφοριών.	ΝΑΙ		
4.10	Θα παρέχεται στοχευμένο re-test για επιβεβαίωση remediation στα ευρήματα που συνέβαλαν στα attack paths.	ΝΑΙ		
4.11	Η τελική αναφορά θα περιλαμβάνει τεχνική ανάλυση, αποτύπωση attack paths και εκτίμηση material business impact.	ΝΑΙ		
4.12	Η αξιολόγηση θα καλύπτει ERP Web Portal με εκτιμώμενες ~400 λειτουργικές οθόνες / διεπαφές.	ΝΑΙ		
4.13	Θα περιλαμβάνεται πλήρης έλεγχος διοικητικής διεπαφής ERP, συμπεριλαμβανομένων privilege escalation paths και segregation-of-duties weaknesses.	ΝΑΙ		
4.14	Ο ανάδοχος θα αποδεικνύει ικανότητα αξιολόγησης περιβάλλοντος AngularJS frontend, ASP.NET Core, IIS/Nginx, Identity Framework και SQL-based backends.	ΝΑΙ		
4.15	Θα αξιολογηθούν μηχανισμοί αυθεντικοποίησης, session lifecycle, token handling και μηχανισμοί invalidation.	ΝΑΙ		
4.16	Θα διερευνηθούν σενάρια login bypass, session hijacking, token replay και fixation.	ΝΑΙ		
4.17	Θα ελεγχθεί η ορθή επιβολή access control μεταξύ ρόλων: Administrator, Human Resource, Payroll, Accounting.	ΝΑΙ		
4.18	Θα αξιολογηθεί δυνατότητα horizontal και vertical privilege escalation μεταξύ ERP ρόλων.	ΝΑΙ		
4.19	Θα διερευνηθούν σενάρια forced browsing και direct request manipulation μεταξύ modules.	ΝΑΙ		
4.20	Θα αξιολογηθούν ~100 διαθέσιμα API methods/endpoints στο πλαίσιο του scope.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.21	Θα αξιολογηθεί η επιβολή object-level και function-level authorization σε επίπεδο API.	ΝΑΙ		
4.22	Θα διερευνηθούν σενάρια parameter tampering και forced manipulation σε επιχειρησιακές λειτουργίες.	ΝΑΙ		
4.23	Θα αξιολογηθούν σενάρια workflow manipulation, approval bypass και κατάχρησης ERP-specific λειτουργιών.	ΝΑΙ		
4.24	Θα διερευνηθούν διαδρομές μη εξουσιοδοτημένης πρόσβασης σε personal, payroll και accounting datasets.	ΝΑΙ		
4.25	Θα αξιολογηθεί κατάχρηση μηχανισμών upload/permissions και πιθανή εκμετάλλευση σχετικής λογικής.	ΝΑΙ		
4.26	Θα αξιολογηθεί υπερβολική επιστροφή δεδομένων μέσω UI ή API (over-exposure / insecure filtering).	ΝΑΙ		
4.27	Θα τεκμηριωθεί συνδυασμός χαμηλής/μεσαίας σοβαρότητας αδυναμιών σε ρεαλιστικά compromise paths υψηλού επιχειρησιακού αντίκτυπου.	ΝΑΙ		
4.28	Δεν επιτρέπονται μη αναστρέψιμες αλλαγές, μαζική εξαγωγή δεδομένων ή disruptive ενέργειες.	ΝΑΙ		
4.29	Η εκμετάλλευση θα περιορίζεται στο απολύτως απαραίτητο για τεκμηρίωση εφικτότητας επίθεσης.	ΝΑΙ		
4.30	Θα τεκμηριώνονται blocks, rate limits και συμπεριφορά αμυντικών μηχανισμών κατά την εκτέλεση σεναρίων.	ΝΑΙ		

ΠΑΡΑΡΤΗΜΑ Γ

ΟΙΚΟΝΟΜΙΚΗ ΠΡΟΣΦΟΡΑ

ΕΤΟΣ*	ΕΤΗΣΙΑ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ (ΧΩΡΙΣ ΦΠΑ) [€]	ΦΠΑ [€]	ΕΤΗΣΙΑ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ (ΜΕ ΦΠΑ) [€]
1ο			
ΣΥΝΟΛΟ			