ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Κτηματολόγιο

Β Τεύχος ερωτήσεων / απαντήσεων

Ηλεκτρονικού Ανοικτού (Διεθνούς) Άνω των Ορίων Διαγωνισμού για το Έργο

«Παροχή Υπηρεσιών Ασφαλείας (Cybersecurity) για την Εγκατάσταση, Παραμετροποίηση και Τεχνική υποστήριξη του εξοπλισμού και των εφαρμογών του ΝΠΔΔ ΕΛΛΗΝΙΚΟ ΚΤΗΜΑΤΟΛΟΓΙΟ»

Ερώτημα 1ο:

Στο πλαίσιο του ως άνω διαγωνισμού και αναφορικά με την απαίτηση της παραγράφου 2.2.6 Τεχνική και επαγγελματική ικανότητα, σύμφωνα με την οποία οι υποψήφιοι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται να διαθέτουν την κατάλληλα τεκμηριωμένη και αποδεδειγμένη επαγγελματική ικανότητα στην υλοποίηση έργων αντίστοιχου μεγέθους και πολυπλοκότητας με το υπό ανάθεση Έργο. Συγκεκριμένα απαιτείται κατά τα τελευταία τρία (3) έτη, από την καταληκτική ημερομηνία υποβολής της προσφοράς του παρόντος διαγωνισμού, είτε αυτοτελώς είτε ως μέλος ένωσης ή κοινοπραξίας είτε ως υπεργολάβος:

«να έχουν ολοκληρώσει τουλάχιστον δέκα (10) έργα συμμόρφωσης με τον Κανονισμό (ΕΕ) 2016/679 (ΓΚΠΔ) ή έργα μελετών εκτίμησης αντικτύπου προστασίας δεδομένων [...], με τουλάχιστον πέντε (5) από αυτά να αφορούν σε πληροφοριακά συστήματα του Δημοσίου τομέα που απευθύνονται σε Έλληνες πολίτες»,

παρακαλούμε όπως διευκρινιστεί το ακόλουθο:

Στην περίπτωση που οικονομικός φορέας έχει αναλάβει αντίστοιχο έργο, η εκτέλεση του οποίου βρίσκεται σε εξέλιξη κατά την καταληκτική ημερομηνία υποβολής των προσφορών, πλην όμως η ολοκλήρωσή του προβλέπεται βάσει του εγκεκριμένου χρονοδιαγράμματος να έχει συντελεστεί σε χρόνο σαφώς προγενέστερο της υπογραφής της σύμβασης του παρόντος διαγωνισμού:

α) Γίνεται δεκτό ο συνυπολογισμός του εν λόγω έργου για την κάλυψη της ανωτέρω απαίτησης;

β) Σε καταφατική περίπτωση, αρκεί προς απόδειξη η υποβολή της απόφασης ανάθεσης και της σχετικής σύμβασης, στις οποίες περιλαμβάνεται και το χρονοδιάγραμμα υλοποίησης του έργου;

Απάντηση:

Έργα που βρίσκονται σε εξέλιξη κατά την καταληκτική ημερομηνία υποβολής προσφορών δεν γίνονται δεκτά για την κάλυψη της απαίτησης, η οποία αφορά ρητά ολοκληρωμένα έργα.

Ερώτημα 2ο:

Στο πλαίσιο του ως άνω διαγωνισμού και για την πληρέστερη ολοκλήρωση της πρότασης μας, ζητούμε την παράταση κατάθεσης των προσφορών κατά 15 ημέρες.

Απάντηση:

Το αίτημα παράτασης λαμβάνεται υπόψη. Η Αναθέτουσα Αρχή θα αποφανθεί εντός των νόμιμων προθεσμιών. Εφόσον χορηγηθεί παράταση, αυτή θα ανακοινωθεί μέσω ΕΣΗΔΗΣ και

θα αφορά το σύνολο των συμμετεχόντων.

Ερώτημα 3ο:

Στην παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα ζητείται ο υποψήφιος να συστήσει Ομάδα Έργου (ΟΕ), με κατ' ελάχιστον την ακόλουθη σύνθεση και τα ακόλουθα προσόντα: «……..

• Ένα (1) Έμπειρο Στέλεχος ασφάλειας πληροφοριακών συστημάτων, με τίτλο σπουδών τριτοβάθμιας εκπαίδευσης (ΑΕΙ/ΤΕΙ) και μεταπτυχιακό τίτλο σπουδών (ένας εκ των δύο τίτλων θα πρέπει να είναι σε θεματική σχετική με πληροφορική), και τουλάχιστον δεκαετή (10) επαγγελματική εμπειρία σε έργα σχετικά με την ασφάλεια πληροφοριακών συστημάτων ή/και με την προστασία προσωπικών δεδομένων, ο οποίος να διαθέτει κατ' ελάχιστον τέσσερις (4) από τις ακόλουθες πιστοποιήσεις: CISA, CISM, CISSP, CDPSE, CIPM. Επιπλέον να διαθέτει κατ’ ελάχιστον τις ακόλουθες πιστοποιήσεις ISO/IEC 27001:2022 Lead Auditor, ISO 22301:2019 Lead Auditor.

…»

Παρακαλούμε να επιβεβαιώσετε ότι η παραπάνω απαίτηση δύναται να καλύπτεται αθροιστικά με τουλάχιστον δύο (2) στελέχη σε ότι αφορά τις πιστοποιήσεις.

Απάντηση:

Δεν επιβεβαιώνεται. Σύμφωνα με τη §2.2.6, ο ρόλος «Έμπειρο Στέλεχος Ασφάλειας Πληροφοριακών Συστημάτων» ορίζεται ως ένα (1) συγκεκριμένο πρόσωπο που πρέπει να συγκεντρώνει αθροιστικά το σύνολο των απαιτούμενων προσόντων και πιστοποιήσεων. Η αθροιστική κάλυψη των πιστοποιήσεων από δύο διαφορετικά πρόσωπα δεν καλύπτει την απαίτηση για τον εν λόγω ρόλο.

Ερώτημα 4ο:

Στην παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα ζητείται ο υποψήφιος να συστήσει Ομάδα Έργου (ΟΕ), με κατ' ελάχιστον την ακόλουθη σύνθεση και τα ακόλουθα προσόντα:

«……..

• Τρία (3) Εξειδικευμένα Στελέχη, με τίτλο σπουδών τριτοβάθμιας εκπαίδευσης (ΑΕΙ/ΤΕΙ) και μεταπτυχιακό τίτλο σπουδών (ένας εκ των δύο τίτλων θα πρέπει να είναι σε θεματική σχετική με πληροφορική), και τουλάχιστον επταετή (7) επαγγελματική εμπειρία σε έργα σχετικά με την ασφάλεια πληροφοριακών συστημάτων ή/και με την προστασία προσωπικών δεδομένων. Τα εν λόγω στελέχη θα πρέπει να διαθέτουν κατ' ελάχιστον τρεις (3) από τις ακόλουθες πιστοποιήσεις: CISA, CISM, CISSP, CDPSE, CIPM, ISO/IEC 27001:2022 Lead Auditor, ISO 22301:2019 Lead Auditor. …» Παρακαλούμε να επιβεβαιώσετε ότι η παραπάνω απαίτηση δύναται να καλύπτεται αθροιστικά, με τουλάχιστον τρία (3) στελέχη που να καλύπτουν τουλάχιστον τρεις (3) από τις απαιτούμενες πιστοποιήσεις.

Απάντηση:

Δεν επιβεβαιώνεται. Για τον ρόλο «Εξειδικευμένα Στελέχη», η απαίτηση «κατ' ελάχιστον τρεις (3) από τις ακόλουθες πιστοποιήσεις» αφορά κάθε στέλεχος ατομικά, ήτοι κάθε ένα εκ των τριών στελεχών πρέπει να διαθέτει τουλάχιστον τρεις (3) από τις απαιτούμενες πιστοποιήσεις. Δεν αρκεί αθροιστική κάλυψη τριών πιστοποιήσεων από το σύνολο των τριών στελεχών.

Ερώτημα 5ο:

Σε ότι αφορά την παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα παρακαλούμε να επιβεβαιώσετε ότι κάποιο στέλεχος της ομάδας μπορεί να καλύψει μέχρι δύο (2) θέσεις όπως αναφέρεται η διακήρυξη και στο τμήμα των έργων «Ένα έργο μπορεί να καλύπτει ταυτόχρονα περισσότερες της μιας από τις παραπάνω κατηγορίες.»

Απάντηση:

Σε αντίθεση με τον όρο "Ένα έργο μπορεί να καλύπτει ταυτόχρονα περισσότερες της μιας από τις παραπάνω κατηγορίες", το οποίο είναι λογικό για την απόδειξη εμπειρίας του Αναδόχου σε παρόμοια έργα, τα προτεινόμενα στελέχη πρέπει να είναι διακριτά και να καλύπτουν από μία θέση στα πλαίσια της Ομάδας Έργου. Με δεδομένο το μέγεθος και την πολυπλοκότητα του έργου δεν επιτρέπεται η κάλυψη δύο (2) θέσεων από το ίδιο στέλεχος.

Ερώτημα 6ο:

Στην παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα ζητείται: «…Για την τεκμηρίωση της Τεχνικής Ικανότητας η αναθέτουσα αρχή κάνοντας χρήση των όρων του «Μέρους ΙΙ του Παραρτήματος XII του Προσαρτήματος Α΄ του Ν.4412/16» λαμβάνει υπόψη και στοιχεία επιτυχώς ολοκληρωμένων έργων που παραδόθηκαν κατά τα τελευταία πέντε (5) έτη από την καταληκτική ημερομηνία υποβολής προσφορών..» Παρακαλούμε να επιβεβαιώσετε ότι η παραπάνω περίοδος αφορά, από 1/1/2021 έως και την καταληκτική ημερομηνία υποβολή προσφορών στις 6/7/2026.

Απάντηση:

Αφορά την τελευταία πενταετία, ήτοι την περίοδο από 6/7/2021 έως 6/7/2026. Εφόσον υπάρξει παράταση την καταληκτική ημερομηνία υποβολής προσφορών, το παραπάνω διάστημα προσαρμόζεται αναλόγως.

Ερώτημα 7ο:

Στην παράγραφο Β.4. Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6 οι οικονομικοί φορείς προσκομίζουν: Α) Κατάλογο με τα κυριότερα συναφή έργα…. Α2) Αν ο αποδέκτης είναι ιδιωτικός φορέας, η παροχή θα αποδεικνύεται με βεβαίωση / δήλωση του αποδέκτη ή υπεύθυνη δήλωση του υποψήφιου οικονομικού φορέα, εφόσον δεν είναι δυνατή η προσκόμιση της βεβαίωσης, και την προσκόμιση της σχετικής έγγραφης Σύμβασης (αντίγραφο) (όπου κι εδώ από τα αναγραφόμενα θα πρέπει να συμπεραίνονται τα παραπάνω στοιχεία του σημείου Α). Παρακαλούμε να επιβεβαιώσετε ότι η προσκόμιση της σχετικής έγγραφης Σύμβασης (αντίγραφο) σε ιδιωτικό έργο απαιτείται και στις 2 περιπτώσεις (είτε

προσκομιστεί δήλωση του αποδέκτη είτε προσκομιστεί υπεύθυνη δήλωση του υποψήφιου οικονομικού φορέα)

Απάντηση:

Το αντίγραφο σύμβασης απαιτείται μόνο εφόσον δεν προσκομίζεται βεβαίωση/δήλωση αποδέκτη, συνοδεύοντας υποχρεωτικά την υπεύθυνη δήλωση του οικονομικού φορέα. Όταν προσκομίζεται βεβαίωση/δήλωση αποδέκτη από την οποία συμπεραίνονται όλα τα απαιτούμενα στοιχεία (αντικείμενο, ημερομηνία ολοκλήρωσης, αξία), το αντίγραφο σύμβασης δεν είναι υποχρεωτικό.

Ερώτημα 8ο:

Στην παράγραφο Β.4. Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6 ζητείται: «….Υπεύθυνη Δήλωση κάθε μέλους της ομάδας έργου περί ακρίβειας των στοιχείων του βιογραφικού σημειώματος τους (δεν απαιτείται το γνήσιο της υπογραφής)….» Παρακαλούμε να διευκρινίσετε αν η ημερομηνία της ΥΔ θα είναι πριν την υποβολή της προσφοράς (6/7/26)

Απάντηση:

Η εν λόγω Υπεύθυνη Δήλωση, της Παρ. 2.2.9.2 αφορά σε Αποδεικτικά μέσα - Δικαιολογητικά Προσωρινού αναδόχου, ως εκ τούτου απαιτείται να φέρει ημερομηνία μετά την πρόσκληση υποβολής δικαιολογητικών κατακύρωσης. Ως προς την υπογραφή του, δύναται να υπογραφή μέσω gov.

Ερώτημα 9ο:

Στην παράγραφο 2.3.1 Κριτήριο ανάθεσης η διακήρυξη αναφέρει: «…Κριτήριο Κ1: Εξετάζεται και αξιολογείται η σαφήνεια και η πληρότητα της πρότασης με σκοπό να εκτιμηθεί ο βαθμός κατανόησης του συμβατικού αντικειμένου από τους προσφέροντες ειδικά ως προς τις ιδιαίτερες απαιτήσεις υλοποίησής του…» Παρακούμε να διευκρινίσετε ποιες είναι οι «ιδιαίτερες απαιτήσεις υλοποίησης του έργου»

Απάντηση:

Οι ιδιαίτερες απαιτήσεις υλοποίησης αφορούν τη φύση και το θεσμικό πλαίσιο της λειτουργίας του Φορέα και των πληροφοριών που διαχειρίζονται, και εξηγούνται στην προκήρυξη. Η κατανόηση των απαιτήσεων αυτών είναι μέρος της τεχνικής αξιολόγησης.

Ερώτημα 10ο:

Στην παράγραφο 2.3.1 Κριτήριο ανάθεσης η διακήρυξη αναφέρει: «…Κριτήριο Κ2: Κρίνεται η σαφήνεια και η πληρότητα της προσφοράς του διαγωνιζομένου της μεθοδολογίας που θα εφαρμόσει σε όλα τα στάδια εκτέλεσης του έργου, ως προς την καταλληλότητα της εφαρμογής της σε σχέση με τις ειδικές απαιτήσεις υλοποίησης του έργου….» Παρακαλούμε να διευκρινίσετε ποιες είναι οι «ειδικές απαιτήσεις υλοποίησης του έργου»

Απάντηση:

Οι ιδιαίτερες απαιτήσεις υλοποίησης αφορούν τη φύση και το θεσμικό πλαίσιο της λειτουργίας του Φορέα και των πληροφοριών που διαχειρίζονται, και εξηγούνται στην προκήρυξη. Η κατανόηση των απαιτήσεων αυτών είναι μέρος της τεχνικής αξιολόγησης.

Ερώτημα 11ο:

Υπάρχουν στην διακήρυξη πολλές συγκεκριμένες αναφορές(σελ.99) σε: • Entra ID / Azure AD • Microsoft Purview Sensitivity Labels • Exchange, SharePoint, OneDrive Επίσης σε ορισμένα σημεία αναφέρεται και Oracle OCI ως επιλογή οργανισμού. Από τις εν λόγω αναφορές η διακήρυξη καταδεικνύει συγκεκριμένους κατασκευαστές. Γίνονται αποδεκτές ισοδύναμες λύσεις άλλων κατασκευαστών με αντίστοιχη λειτουργικότητα;

Απάντηση:

Οι απαιτήσεις συγκεκριμένων συστημάτων διασφαλίζουν τη συμβατότητα με υφιστάμενες υποδομές και συστήματα του Φορέα. Όλες οι τεχνικές προσφορές θα πρέπει να διασφαλίζουν την κάλυψη των συγκεκριμένων απαιτήσεων όπως αναφέρονται στους Πίνακες Συμμόρφωσης της διαχείρισης.

Ερώτημα 12ο:

Σε αρκετές υπηρεσίες αναφέρονται: • guaranteed response times, • guaranteed resolution times, • Απαιτείται SLA compliance με guaranteed response και resolution times (σελ.95), • Απαιτείται flexible engagement model με guaranteed response times. (σελ.96), χωρίς στα ίδια σημεία να προσδιορίζονται ακριβείς χρόνοι. Παρακαλούμε να δοθεί πίνακας SLA ανά κατηγορία περιστατικού (P1-P4), response και resolution times καθώς αποτελεί έλλειψη της διακήρυξης.

Απάντηση:

Οι απαιτήσεις SLA για response / resolution times αναφέρονται συγκεκριμένα στην Προκήρυξη (παράγραφος 3.1.6, σελίδα 99).

Ερώτημα 13ο:

Το Μέρος Β της διακήρυξης αναφέρει ότι απαιτεί τα παρακάτω: • Διεξαγωγή ασκήσεων Risk assessment ασφάλειας πληροφοριών Οι ασκήσεις risk assessment πρέπει να καλύπτουν όλα τα κρίσιμα συστήματα του Κτηματολογίου, να περιλαμβάνουν εντοπισμό απειλών και ευπαθειών, αξιολόγηση αντικτύπου (Σελ.90) και να παράγουν σχέδια δράσης για την αντιμετώπιση των κινδύνων. • Οι ασκήσεις DPIA πρέπει να εκτελούνται για κάθε νέα επεξεργασία δεδομένων ή σημαντική μεταβολή υφιστάμενης επεξεργασίας που ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων. (σελ.91) • Εκτέλεση ασκήσεων και καταγραφή συσχετιζόμενων reports. Οι ασκήσεις penetration testing πρέπει να εκτελούνται από certified ethical hackers, να περιλαμβάνουν black box, white box και gray box testing, να καλύπτουν OWASP Top 10, να παράγουν executive και technical reports με CVSS scoring και να περιλαμβάνουν remediation verification testing. (σελ.93) • Red Team • Compliance Audits • DR Testing αλλά δεν προσδιορίζεται επακριβώς:

• πλήθος ασκήσεων, • πλήθος ελέγχων, • πλήθος εφαρμογών, • πλήθος εγκαταστάσεων. Παρακαλούμε να προσδιοριστεί το αναμενόμενο πλήθος ασκήσεων, ελέγχων, εφαρμογών και υποδομών ανά υπηρεσία.

Απάντηση:

Ο μέγιστος αριθμός ad hoc ασκήσεων για κάθε κατηγορία αναφέρεται στον στήλη «Τεμάχια» του Πίνακα Β.2 της Οικονομικής Προσφοράς, σελ. 162. Λοιπές τεχνικές λεπτομέρειες θα συμφωνηθούν με βάση την προσφορά του αναδόχου.

Ερώτημα 14ο:

Στην προδιαγραφή 6.6.(σελ.110) η διακήρυξη απαιτεί : «…Εγγύηση της διαλειτουργικότητας της υπηρεσίας με όλα τα υφιστάμενα αλλά και τα μελλοντικά συστήματα του κτηματολογίου…» Δεδομένου ότι η οικονομική προσφορά υποβάλλεται σε σταθερή και δεσμευτική βάση κατά το στάδιο του διαγωνισμού, παρακαλούμε να διευκρινισθεί: α) ποια είναι τα υφιστάμενα συστήματα αναφοράς με τα οποία απαιτείται υποχρεωτικά διαλειτουργικότητα κατά την έναρξη του έργου, β) εάν η απαίτηση περί «μελλοντικών συστημάτων» αφορά αποκλειστικά συστήματα όμοιου τεχνολογικού αντικειμένου και προτύπων διασύνδεσης με τα ήδη υφιστάμενα, και ποια μπορεί να είναι, ώστε διασφαλίζεται η συγκρισιμότητα και η ίση μεταχείριση των υποψηφίων αναδόχων στην αξιολόγηση.

Απάντηση:

Η απαίτηση αφορά την δυνατότητα Open Architecture η οποία εγγυάται τη διαλειτουργικότητα της υπηρεσίας μέσω τυπικών προτύπων και διεπαφών (API) με τα υφιστάμενα και μελλοντικά συστήματα του κτηματολογίου. Η απαίτηση «μελλοντικά συστήματα» αφορά συστήματα του ίδιου τεχνολογικού αντικειμένου και προτύπων που θα αναπτυχθούν βάσει αντίστοιχων προτύπων διασύνδεσης - δεν αφορά ριζικά νέες τεχνολογίες που δεν προβλέπονται κατά τη σύναψη της σύμβασης.

Ερώτημα 15ο:

Παρακαλούμε να δοθούν αναλυτικά οι ποσότητες assets που θα ενταχθούν στις υπηρεσίες MDR (endpoints, servers, cloud resources, network devices, applications).

Απάντηση:

Περαιτέρω λεπτομέρειες και αναλυτικά στοιχεία θα παρασχεθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 16ο:

Στην προδιαγραφή 1.4.(σελ.110) η διακήρυξη απαιτεί για την ΥΠΗΡΕΣΙΑ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΑΠΟΚΡΙΣΗΣ (MANAGED DETECTION AND RESPONSE) : Κατ' ελάχιστο να υποστηρίζονται Microsoft Defender. Επιτρέπεται η χρήση ισοδύναμων EDR/XDR πλατφορμών άλλων κατασκευαστών εφόσον διασφαλίζεται πλήρης λειτουργική ισοδυναμία;

Απάντηση:

Η απαίτηση αφορά την εμπειρία και τεχνογνωσία του Αναδόχου στην υποστήριξη Microsoft Defender, και είναι ζητούμενο για λόγους συμβατότητας με υφιστάμενα συστήματα. Η απαίτηση «κατ' ελάχιστον να υποστηρίζονται Microsoft Defender» ορίζει ελάχιστη απαίτηση υποστήριξης και όχι αποκλειστική χρήση. Ισοδύναμες EDR/XDR πλατφόρμες άλλων κατασκευαστών γίνονται αποδεκτές, εφόσον καλύπτουν πλήρως τις προδιαγραφές του Πίνακα Συμμόρφωσης Α.3, τεκμηριώνεται η πλήρης λειτουργική ισοδυναμία με Microsoft Defender και διασφαλίζεται ενοποίηση με το περιβάλλον του φορέα.

Ερώτημα 17ο:

Στην σελίδα 99 (παρ.3.1.6) της διακήρυξης αναφέρεται η παρακάτω απαίτηση: «….Κατά την διάρκεια παροχής των υπηρεσιών υποστήριξης, ο σύμβουλος οφείλει να ανταποκρίνεται σε ζητήματα (SLA) ανάλογα με τη φύση και την κρισιμότητα τους ως εξής: ο High importance. 30 min response – 2 hours fix. Αφορά θέματα μερικής μη λειτουργίας του συστήματος ή ορισμένων δυνατοτήτων αυτού. ο Medium importance. 1 hour response – 24 hours fix. Αφορά θέματα μερικής μη λειτουργίας ορισμένων λειτουργικοτήτων. ο Low importance. 4 hours response - 48 hours fix. Αφορά θέματα που δεν επηρεάζουν τη λειτουργία αλλά δυσχεραίνουν την αποδοτικότητα αυτής. ο No importance. 1 day response – 5 days fix. Αφορά όλα τα λοιπά θέματα….» Παρακαλούμε να διευκρινίσετε το παρακάτω και αν χρειάζεται τροποποίηση η διακήρυξη: Οι αναφερόμενοι χρόνοι αφορούν χρόνο πρώτης απόκρισης ή πλήρους αποκατάστασης; Υπολογίζονται σε ημερολογιακό ή εργάσιμο χρόνο;

Απάντηση:

Οι αναφερόμενοι χρόνοι αφορούν ημερολογιακό χρόνο.

Ερώτημα 18ο:

Στην προδιαγραφή 6.4 (σελ.109) της διακήρυξης απαιτείται: «…Τα τελικά KPIs θα καθορισθούν κατά την μελέτη εφαρμογής.» Αυτό δημιουργεί συμβατικό κίνδυνο καθώς ο υποψήφιος ανάδοχος αναλαμβάνει υποχρεώσεις χωρίς να γνωρίζει τα τελικά KPI. Παρακαλούμε να δοθούν τα ελάχιστα αποδεκτά KPI που θα αποτελέσουν συμβατική υποχρέωση του Αναδόχου ώστε διασφαλίζεται η συγκρισιμότητα και η ίση μεταχείριση των υποψηφίων αναδόχων στην αξιολόγηση.

Απάντηση:

Τα ενδεικτικά KPIs που αναφέρονται στην προδιαγραφή 6.4 είναι και τα ελάχιστα αποδεκτά. Ο Ανάδοχος μπορεί στην τεχνική προσφορά να προτείνει τεκμηριωμένα εκείνα τα επιπλέον KPIs που θεωρεί σημαντικά για την παρακολούθηση των παρεχόμενων υπηρεσιών.

Ερώτημα 19ο:

Στην σελίδα 7 η διακήρυξη αναφέρει: «…Ένα τμήμα των υπηρεσιών (βλ. Β.2 της οικονομικής προσφοράς), παρόλο που αξιολογείται και λαμβάνεται υπόψη στην τεχνική και οικονομική προσφορά του οικονομικού φορέα και περιλαμβάνεται στον προϋπολογισμό του έργου, είναι προαιρετικό και μπορεί να υλοποιηθεί σε οποιοδήποτε ποσοστό κρίνει το ΕΛΛΗΝΙΚΟ

ΚΤΗΜΑΤΟΛΟΓΙΟ κατά την ελεύθερη κρίση του.» Επίσης στην σελίδα 85 αναφέρει: Β.2. Ad-hoc παροχή υπηρεσιών, που θα παρέχονται κατά παραγγελία από τον Φορέα, όποτε αυτές απαιτούνται, με το μέσο κόστος που έχει δοθεί από τον Ανάδοχο στην Οικονομική του προσφορά, για το συγκεκριμένο είδος υπηρεσιών.» Δεδομένου ότι το Β.2 είναι προαιρετικό και δύναται να μην ενεργοποιηθεί, παρακαλούμε να διευκρινιστεί αν η οικονομική αξιολόγηση γίνεται με ή χωρίς το ποσό του Β.2 και ποιος είναι ο ελάχιστος εγγυημένος όγκος ενεργοποίησης.

Απάντηση:

Η οικονομική αξιολόγηση περιλαμβάνει το ποσό Β.2, καθώς αυτό αποτελεί μέρος του συνολικού προϋπολογισμού και αξιολογείται τεχνικά και οικονομικά. Η προαιρετικότητα αφορά τον βαθμό ενεργοποίησής του κατά τη διάρκεια εκτέλεσης της σύμβασης, όχι την εξαίρεσή του από την αξιολόγηση.

Δεν ορίζεται ελάχιστος εγγυημένος όγκος ενεργοποίησης Β.2. Το Κτηματολόγιο δύναται να ενεργοποιήσει το Β.2 σε οποιοδήποτε ποσοστό (0–100%) κατά την ελεύθερη κρίση του. Ο Ανάδοχος δεν δικαιούται αποζημίωση για μη ενεργοποίηση υπηρεσιών Β.2.

Ερώτημα 20ο:

Παρατηρούμε ότι σε διάφορα σημεία της Διακήρυξης και ιδιαίτερα στις τεχνικές προδιαγραφές περιλαμβάνονται εκτενείς παράγραφοι, απαιτήσεις και περιγραφές υπηρεσιών στην αγγλική γλώσσα. Δεδομένου ότι η Διακήρυξη αποτελεί διοικητικό έγγραφο που διέπει τη διαδικασία ανάθεσης και ότι τυχόν διαφορετικές ερμηνείες των αγγλικών όρων ενδέχεται να επηρεάσουν τη σύνταξη και αξιολόγηση των προσφορών, παρακαλούμε να χορηγηθεί επίσημη μετάφραση στην ελληνική γλώσσα των αγγλόφωνων παραγράφων της Διακήρυξης ή να διευκρινισθεί ποιο κείμενο υπερισχύει σε περίπτωση διαφορετικής ερμηνείας μεταξύ της αγγλικής και της ελληνικής διατύπωσης, προκειμένου να διασφαλισθεί η ομοιόμορφη κατανόηση των απαιτήσεων από όλους τους οικονομικούς φορείς και η ίση μεταχείριση κατά την προετοιμασία των προσφορών. Παρακαλούμε να επιβεβαιωθεί ότι σε περίπτωση ερμηνευτικής απόκλισης μεταξύ ελληνικού και αγγλικού κειμένου υπερισχύει το ελληνικό κείμενο της Διακήρυξης.

Απάντηση:

Οι αγγλικοί όροι και οι αγγλικές διατυπώσεις έχουν χρησιμοποιηθεί αποκλειστικά ως διεθνώς καθιερωμένη τεχνική ορολογία και λειτουργίες και δεν παραπέμπουν σε συγκεκριμένα προϊόντα ή εμπορικές ονομασίες.

Επιβεβαιώνεται ότι σε περίπτωση ασάφειας ή διαφορετικής ερμηνείας μεταξύ ελληνικής και αγγλικής διατύπωσης, η συμμόρφωση θα αξιολογηθεί με βάση την ουσιαστική τεχνική λειτουργικότητα που ζητείται και όχι με βάση συγκεκριμένη ονομασία, εμπορική διατύπωση ή ακριβή λεκτική αντιστοίχιση αγγλικού όρου.

Τέλος, επιβεβαιώνεται ότι γίνονται αποδεκτές ισοδύναμες τεχνικές προσεγγίσεις, εφόσον ο προσφέρων τεκμηριώνει ότι καλύπτουν πλήρως το λειτουργικό αποτέλεσμα που περιγράφεται στις σχετικές προδιαγραφές.

Ερώτημα 21ο:

Σχετικά με την λύση Α.1. IDM/IAM/Multi- Factor Authentication (MFA) Αναφέρεται το εξης : Η προτεινόμενη λύση να περιλαμβάνει τις άδειες που να καλύπτουν τουλάχιστον τους ζητούμενους χρήστες του οργανισμού. >= 2700. Παρακαλούμε να διευκρινιστεί εάν αφορά την προμήθεια των αδειών και το κόστος τους για 2700 χρήστες για 3 έτη.

Απάντηση:

Ναι επιβεβαιώνεται.

Ερώτημα 22ο:

Σχετικά με την λύση Α.3. END POINT SECURITY Αναφέρεται το εξης : Η προτεινόμενη λύση να περιλαμβάνει τις άδειες που να καλύπτουν τουλάχιστον τους ζητούμενους χρήστες του οργανισμού. >= 2700. Παρακαλούμε να διευκρινιστεί εάν αφορά την προμήθεια των αδειών και το κόστος τους για 2700 χρήστες για 3 έτη.

Απάντηση:

Ναι επιβεβαιώνεται.

Ερώτημα 23ο:

Στην παράγραφο 2.2.6 «Τεχνική και επαγγελματική ικανότητα» προβλέπεται ότι για το Έμπειρο Στέλεχος Ασφάλειας Πληροφοριακών Συστημάτων απαιτείται:

- η κατοχή κατ' ελάχιστον τεσσάρων (4) εκ των πιστοποιήσεων CISA, CISM, CISSP, CDPSE, CIPM, και
- επιπλέον η κατοχή των πιστοποιήσεων ISO/IEC 27001:2022 Lead Auditor και ISO 22301:2019 Lead Auditor.

Ωστόσο, η διατύπωση αυτή είναι αόριστη και επιδεκτική διαφορετικών ερμηνειών, καθώς δεν προκύπτει με σαφήνεια:

- εάν απαιτούνται τέσσερις (4) εκ των επτά (7) συνολικά πιστοποιήσεων, ή
- εάν απαιτούνται τέσσερις (4) εκ των πέντε (5) πρώτων, σωρευτικά με την υποχρεωτική κατοχή των δύο ISO Lead Auditor.

Επιπλέον, δεν αποσαφηνίζεται εάν τα ανωτέρω προσόντα πρέπει να συντρέχουν στο ίδιο φυσικό πρόσωπο ή μπορούν να καλύπτονται από περισσότερα μέλη της Ομάδας Έργου.

Η ασάφεια αυτή επηρεάζει ουσιωδώς το επίπεδο τεχνικής απαίτησης και ενδέχεται να εισάγει δυσανάλογο περιορισμό του ανταγωνισμού.

Κατόπιν των ανωτέρω, ζητείται:

1. Να διευκρινιστεί ρητά η ακριβής απαίτηση ως προς τον αριθμό και το συνδυασμό των πιστοποιήσεων.

2. Να επιβεβαιωθεί εάν οι απαιτούμενες πιστοποιήσεις δύνανται να καλύπτονται αθροιστικά από περισσότερα μέλη της Ομάδας Έργου.

3. Σε διαφορετική περίπτωση, να παρατεθεί σχετική αιτιολόγηση ή/και να εξεταστεί η τροποποίηση της απαίτησης.

Απάντηση:

Οι απαιτήσεις για το Έμπειρο Στέλεχος ασφάλειας πληροφοριακών συστημάτων ορίζονται σαφώς ως «κατ'ελάχιστον τέσσερεις (4) από τις ακόλουθες πιστοποιήσεις: CISA, CISM, CISSP, CDPSE, CIPM, και ΕΠΙΠΛΕΟΝ να διαθέτει κατ' ελάχιστον τις ακόλουθες πιστοποιήσεις ISO/IEC 27001:2022 Lead Auditor, ISO 22301:2019 Lead Auditor.

Αρα οι απαιτήσεις αφορούν κατ' ελάχιστον 6 πιστοποιήσεις (4 εκ 5 + 2 υποχρεωτικές ISO), που πρέπει να συντρέχουν στο ίδιο φυσικό πρόσωπο.

Για λόγους συνοχής της ομάδας έργου και απαιτήσεων συνδυασμένης εμπειρίας οι εν λόγω απαιτήσεις θα πρέπει να καλύπτονται όλες από το ίδιο στέλεχος. Δεν αρκεί να καλύπτονται από διαφορετικά στελέχη καθώς αποτελούν συμπληρωματικές γνώσεις και εμπειρία που πρέπει να παρέχονται συνδυαστικά από το συγκεκριμένο Έμπειρο Στέλεχος.

Ερώτημα 24ο:

Στην ίδια παράγραφο προβλέπεται η συμμετοχή τριών (3) εξειδικευμένων στελεχών, τα οποία πρέπει να διαθέτουν κατ' ελάχιστον τρεις (3) από συγκεκριμένες πιστοποιήσεις.

Ωστόσο, δεν αποσαφηνίζεται εάν η απαίτηση αυτή αφορά:

- κάθε στέλεχος ατομικά, ή
- τη συνολική κάλυψη των πιστοποιήσεων σε επίπεδο Ομάδας Έργου.

Η ασάφεια αυτή οδηγεί σε διαφορετικά επίπεδα τεχνικής απαίτησης και επηρεάζει την συγκρισιμότητα των προσφορών.

Κατόπιν των ανωτέρω, ζητείται:

1. Να διευκρινιστεί εάν η απαίτηση κατοχής των τριών (3) πιστοποιήσεων αφορά κάθε στέλεχος χωριστά ή την Ομάδα συνολικά.

2. Να επιβεβαιωθεί εάν επιτρέπεται η αθροιστική κάλυψη των πιστοποιήσεων από τα τρία στελέχη.

3. Σε διαφορετική περίπτωση, να αιτιολογηθεί η σχετική απαίτηση ή/και να εξεταστεί η αναθεώρησή της.

Απάντηση:

Η απαίτηση αφορά κάθε στέλεχος ατομικά. Για λόγους συνοχής της ομάδας έργου και αναγκών για πλήθος τριών (3) στελεχών με τη σχετική εμπειρία οι εν λόγω απαιτήσεις θα πρέπει να καλύπτονται ξεχωριστά από κάθε ένα από τα τρία στελέχη της ομάδας έργου.

Ερώτημα 25ο:

Σε σχέση με τη συγκρότηση της Ομάδας Έργου, δεν προκύπτει με σαφήνεια εάν επιτρέπεται η κάλυψη περισσότερων του ενός ρόλων από το ίδιο στέλεχος.

Παράλληλα, στη διακήρυξη προβλέπεται ότι «ένα έργο μπορεί να καλύπτει ταυτόχρονα περισσότερες της μίας κατηγορίες», γεγονός που δημιουργεί εύλογη αναλογία ως προς τη δυνατότητα πολλαπλής αξιοποίησης της εμπειρίας και σε επίπεδο στελεχών.

Η έλλειψη ρητής πρόβλεψης δημιουργεί ασάφεια ως προς τη στελέχωση και ενδέχεται να επηρεάσει την ισότιμη αξιολόγηση των προσφορών.

Κατόπιν των ανωτέρω, ζητείται:

1. Να διευκρινιστεί εάν επιτρέπεται ένα στέλεχος να καλύπτει περισσότερους του ενός ρόλους (έως δύο), εφόσον πληροί τα απαιτούμενα προσόντα.

2. Να επιβεβαιωθεί η δυνατότητα πολλαπλής αξιοποίησης της εμπειρίας και των προσόντων στελέχους σε περισσότερες θέσεις της Ομάδας Έργου.

3. Σε διαφορετική περίπτωση, να παρατεθεί σχετική αιτιολόγηση ή/και να εξεταστεί η αποσαφήνιση της διακήρυξης.

Απάντηση:

Σε αντίθεση με τον όρο "Ένα έργο μπορεί να καλύπτει ταυτόχρονα περισσότερες της μιας από τις παραπάνω κατηγορίες", το οποίο είναι λογικό για την απόδειξη εμπειρίας του Αναδόχου σε παρόμοια έργα, τα προτεινόμενα στελέχη πρέπει να είναι διακριτά και να καλύπτουν από μία θέση στα πλαίσια της Ομάδας Έργου. Με δεδομένο το μέγεθος και την πολυπλοκότητα του έργου δεν επιτρέπεται η κάλυψη δύο (2) θέσεων από το ίδιο στέλεχος.

Ερώτημα 26ο:

Παρακαλούμε όπως επιβεβαιώσετε πως οι απαιτούμενες άδειες λογισμικού Microsoft Entra ID Governance θα είναι διαθέσιμες από την Αναθέτουσα Αρχή για το σύνολο των χρηστών (1.900 χρήστες) που εμπίπτουν στις απαιτούμενες υπηρεσίες υλοποίησης που αναγράφονται στην ενότητα 3.1.2.1 Α.1 Identity & Access Management και ότι δεν απαιτείται η προμήθεια των αδειών αυτών από τον Ανάδοχο, καθώς δεν υπάρχει σχετική απαίτηση στην ενότητα 3.1.5. Δ. ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΕΣ ΛΥΣΕΙΣ και τους αντίστοιχους πίνακες της οικονομικής προσφοράς.

Απάντηση:

Βλέπε απάντηση ερωτήματος 21 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 27ο:

Παρακαλούμε όπως επιβεβαιώσετε πως οι απαιτούμενες άδειες λογισμικού Microsoft Purview (είτε μέσω standalone Purview Licensing Suite, είτε Microsoft E5, είτε παρεμφερούς licensing scheme) θα είναι διαθέσιμες από την Αναθέτουσα Αρχή για το σύνολο των χρηστών (1.900 χρήστες) που εμπίπτουν στις απαιτούμενες υπηρεσίες υλοποίησης που αναγράφονται στην ενότητα 3.1.2.2 Προστασία Δεδομένων – και συγκεκριμένα στις παραγράφους Data Loss Prevention (DLP) και Data Classification – και ότι δεν απαιτείται η προμήθεια των αδειών αυτών από τον Ανάδοχο, καθώς δεν υπάρχει σχετική απαίτηση στην ενότητα 3.1.5. Δ.

ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΕΣ ΛΥΣΕΙΣ και τους αντίστοιχους πίνακες της οικονομικής προσφοράς.

Απάντηση:

Βλέπε απάντηση ερωτήματος 22 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 28ο:

Ομοίως με τα Ερωτήματα 1 & 2 παρακαλούμε όπως επιβεβαιώσετε πως υφίσταται λύση και σχετικές άδειες λογισμικού Database Protection & Κρυπτογράφηση Δεδομένων, καθώς οι απαιτούμενες υπηρεσίες υλοποίησης που αναγράφονται στην ενότητα 3.1.2.2 Προστασία Δεδομένων – και συγκεκριμένα στην παράγραφο Database Protection – και ότι δεν απαιτείται η προμήθεια της λύσης και των σχετικών αδειών από τον Ανάδοχο, καθώς δεν υπάρχει σχετική απαίτηση στην ενότητα 3.1.5. Δ. ΛΟΓΙΣΜΙΚΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΕΣ ΛΥΣΕΙΣ και τους αντίστοιχους πίνακες της οικονομικής προσφοράς.

Απάντηση:

Βλέπε απάντηση ερωτήματος 23 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 29ο:

Παρακαλούμε να διευκρινιστεί σε ποιο σημείο θα πρέπει ο Ανάδοχος να δηλώσει την τιμή για την απαίτηση «Αναθεώρηση ή ανάπτυξη της μεθοδολογίας Αξιολόγησης και Διαχείρισης Κινδύνων Ασφάλειας Πληροφοριών» που αναγράφεται στην ενότητα 3.1.3.4. Β.2.1 Διαχείριση Κινδύνων & Αξιολόγηση, καθώς η ανάπτυξη της μεθοδολογίας αποτελεί ξεχωριστό παραδοτέο (βλ. ενότητα 3.5.2. Παραδοτέα Σύμβασης - Β.2 Ad-hoc Παροχή Υπηρεσιών - Β.2.1 Risk Management -Μεθοδολογία) και προηγείται της διεξαγωγής των ασκήσεων, για τις οποίες καλείται ο Ανάδοχος να δηλώσει τις αντίστοιχες τιμές στον πίνακα οικονομικής προσφοράς ανά άσκηση.

Απάντηση:

Βλέπε απάντηση ερωτήματος 24 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 30ο:

Παρακαλούμε να διευκρινιστεί σε ποιο σημείο θα πρέπει ο Ανάδοχος να δηλώσει την τιμή για τις απαιτήσεις «Ανάπτυξη Στρατηγικής Επιχειρησιακής Συνέχειας», «Ανάπτυξη Πλάνων Επιχειρησιακής Συνέχειας», «Ανάπτυξη Πολιτικής Επιχειρησιακής Συνέχειας» και «Crisis Management Procedures» που αναγράφονται στην ενότητα 3.1.3.5. Β.2.2 Business Impact Analysis (ανάπτυξη BCP & DRP περιλαμβ. BIA), καθώς τα σχετικά έγγραφα αποτελούν ξεχωριστά παραδοτέα (βλ. ενότητα 3.5.2. Παραδοτέα Σύμβασης - Β.2 Ad-hoc Παροχή Υπηρεσιών - Β.2.2 Business Impact Analysis - Business Continuity Strategy & Plans, BC Policy, Crisis Management) από τις ασκήσεις Business Impact Assessment (BIA) , για τις οποίες καλείται ο Ανάδοχος να δηλώσει τις αντίστοιχες τιμές στον πίνακα οικονομικής προσφοράς ανά άσκηση.

Απάντηση:

Βλέπε απάντηση ερωτήματος 25 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 31ο:

Παρακαλούμε να επιβεβαιωθεί ότι η απαίτηση «Δοκιμές Αποκατάστασης & Drills» στην ενότητα 3.1.3.9. Β.2.6. Δοκιμές αποκατάστασης και drills δεν αποτελεί ξεχωριστή απαίτηση από τις «Δοκιμές Disaster Recovery» στην ενότητα 3.1.4.3. Γ.3 Backup and DR Management.

Απάντηση:

Βλέπε απάντηση ερωτήματος 26 Α τεύχους ερωτήσεων/ απαντήσεων.

Πρόκειται για δύο διακριτές απαιτήσεις που δεν ταυτίζονται:

- Β.2.6 (§3.1.3.9): Ad-hoc drills και ασκήσεις BC/DR που παραγγέλλονται κατά διαστήματα από τον Φορέα και τιμολογούνται ανά άσκηση (Πίνακας Β.2).
- Γ.3 (§3.1.4.3): Τακτικές Δοκιμές Disaster Recovery (quarterly) που αποτελούν μέρος της συνεχούς υπηρεσίας επίβλεψης του Backup & DR Management τιμολογούνται στο Μέρος Γ.

Ερώτημα 32ο:

Παρακαλούμε να επιβεβαιωθεί ότι για τους ρόλους «Έμπειρο Στέλεχος Ασφάλειας Πληροφοριακών Συστημάτων» και «Εξειδικευμένα Στελέχη» όπου ζητείται μεταξύ άλλων η πιστοποίηση ISO/IEC 27001:2022 Lead Auditor, η απαίτηση δύναται να καλυφθεί και μέσω της πιστοποίησης ISO/IEC 27001:2013 Lead Auditor, η οποία είναι ισοδύναμη και αφορά στο ίδιο πρότυπο.

Απάντηση:

Βλέπε απάντηση ερωτήματος 27 πρώτου τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 33ο:

Παρακαλούμε να διευκρινιστεί ο συνολικός αριθμός των χρηστών της πλατφόρμας εκπαίδευσης, καθώς σε κάποια σημεία της διακήρυξης αναφέρεται ο αριθμός 3.000 και σε κάποια άλλα σημεία ο αριθμός 1.900.

Απάντηση:

Βλέπε απάντηση ερωτήματος 28 πρώτου τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 34ο:

Παρακαλούμε όπως επιβεβαιώσετε ότι η σύμβαση δεν υποδιαιρείται σε τμήματα βάσει της αναφοράς της §1.3 της διακήρυξης: [...] Το αντικείμενο της παρούσας σύμβασης δεν υποδιαιρείται σε τμήματα, [...]. Ως εκτούτου η αναφορά στο τέλος της ίδιας παραγράφου έχει μπει εκ παραδρομής: [...] Η σύμβαση έχει υποδιαιρεθεί σε δύο (2) Τμήματα, το ένα (1) εκ των οποίων θα ανατεθεί με προσφυγή στην παρέκκλιση της παρ. 10 του άρθρου 6 του

4412/2016, σύμφωνα και με την υπ' αριθμ. 381/12/06.11.2025 Απόφαση Διοικητικού Συμβουλίου.

Απάντηση:

Βλέπε απάντηση ερωτήματος 29 πρώτου τεύχους ερωτήσεων απαντήσεων.

Ερώτημα 35ο:

Στην § 2.2.9.2 Αποδεικτικά μέσα - Δικαιολογητικά προσωρινού αναδόχου, σημείο Α της διακήρυξης μεταξύ άλλων, αναφέρεται: «Τα αποδεικτικά μέσα του παρόντος που γίνονται αποδεκτά κατά την παρ. 12 του άρθρου 80 του ν. 4412/2016 θεωρείται ότι ισχύουν και κατά τον χρόνο υπογραφής του Ευρωπαϊκού Ενιαίου Έγγραφου Σύμβασης (Ε.Ε.Ε.Σ.) του άρθρου 79, εκτός αν η αναθέτουσα αρχή, αυτεπαγγέλτως, ή έτερος οικονομικός φορέας που συμμετέχει στην οικεία διαδικασία ανάθεσης σύμβασης, με την άσκηση προσφυγής σύμφωνα με το Βιβλίο IV του ως άνω νόμου, αποδείξει ότι τα αναφερόμενα σε αυτά δεν ίσχυαν κατά τον χρόνο υπογραφής του Ε.Ε.Ε.Σ..».

Στην ίδια § σημείο Β, μεταξύ άλλων, αναφέρεται: «Οι οικονομικοί φορείς μεριμνούν να διαθέτουν πιστοποιητικά, τα οποία να καλύπτουν και τον χρόνο υποβολής της προσφοράς, προκειμένου να τα υποβάλουν, εφόσον αναδειχθούν προσωρινοί ανάδοχοι. Τα εν λόγω πιστοποιητικά υποβάλλονται μαζί με τα υπόλοιπα αποδεικτικά μέσα της παραγράφου 3.2 της παρούσας, από τον προσωρινό ανάδοχο, με επισύναψη των σχετικών στοιχείων στον (υπο) φάκελο της ηλεκτρονικής περιοχής της απάντησής του «Δικαιολογητικά Κατακύρωσης».

Παρακαλούμε όπως επιβεβαιώσετε ότι τα πιστοποιητικά, τα οποία καλύπτουν και τον χρόνο υποβολής της προσφοράς, δεν απαιτείται να υποβληθούν κατά το στάδιο υποβολής των δικαιολογητικών του προσωρινού αναδόχου.

Απάντηση:

Βλέπε απάντηση ερωτήματος 30 πρώτου τεύχους ερωτήσεων απαντήσεων.

Ερώτημα 36ο:

Σύμφωνα με την § 2.2.9.1 Προκαταρκτική απόδειξη κατά την υποβολή προσφορών της Διακήρυξης «Προς προκαταρκτική απόδειξη ότι οι προσφέροντες οικονομικοί φορείς: α) δεν βρίσκονται σε μία από τις καταστάσεις της § 2.2.3 «Λόγοι Αποκλεισμού» και β) πληρούν τα «Κριτήρια Ποιοτικής Επιλογής» των § 2.2.4, 2.2.5, 2.2.6 και 2.2.7 της παρούσης, προσκομίζουν κατά την υποβολή της προσφοράς τους ως δικαιολογητικό συμμετοχής, το προβλεπόμενο από το άρθρο 79 παρ. 1 και 3 του ν. 4412/2016 Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης (ΕΕΕΣ), σύμφωνα με το επισυναπτόμενο στην παρούσα ΠΑΡΑΡΤΗΜΑ ΙΙ – ΕΥΡΩΠΑΪΚΟ ΕΝΙΑΙΟ ΕΓΓΡΑΦΟ ΣΥΜΒΑΣΗΣ (ΕΕΕΣ), το οποίο ισοδυναμεί με ενημερωμένη υπεύθυνη δήλωση, με τις συνέπειες του ν. 1599/1986. Το ΕΕΕΣ καταρτίζεται βάσει του τυποποιημένου εντύπου του Παραρτήματος 2 του Κανονισμού (ΕΕ) 2016/7, συμπληρώνεται από τους προσφέροντες οικονομικούς φορείς σύμφωνα με τις οδηγίες του Παραρτήματος 1».

Περαιτέρω, σύμφωνα με τα αρχεία του ΕΕΣΣ σε pdf και xml μορφή τα οποία βρίσκονται αναρτημένα στην Πλατφόρμα

https://protect.checkpoint.com/v2/r02/___www.promitheus.gov.gr___.YzJlOmFkYWNvbW5ldDpjOm86MGJiMTFkODgwZmZiZDliMzk5MmZmNWEzNjU1YWFmZWQ6NzpmYzkwOjlhMGE5MGQyNDYwNWNkMjQ5MjJjZDhkMWZmNzAxOThiNzYyM2E1ZWFiOWQyY2YxZmFlMmVmZDJmYjQ4ZDJiYmU6dDpGOk4 καθώς και στον χώρο «ΣΗΜΕΙΩΣΕΙΣ & ΣΥΝΗΜΜΕΝΑ» του διαγωνισμού με συστημικό αριθμό ΕΣΗΔΗΣ: 421023 στο Μέρος IV Κριτήρια επιλογής του ΕΕΕΣ δίνεται η δυνατότητα συμπλήρωσης μόνο της ενότητας α «Γενική ένδειξη για όλα τα κριτήρια επιλογής».

Δεδομένου ότι εντός του τυποποιημένου εντύπου του Παραρτήματος 2 του Κανονισμού (ΕΕ) 2016/7 του ΕΕΕΣ στο Μέρος IV: Κριτήρια επιλογής τα πεδία είναι ενεργά προς συμπλήρωση για κάθε κριτήριο επιλογής (Α. ΚΑΤΑΛΛΗΛΟΤΗΤΑ, Β. ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗ ΕΠΑΡΚΕΙΑ, Γ. ΤΕΧΝΙΚΗ ΚΑΙ ΕΠΑΓΓΕΛΜΑΤΙΚΗ ΙΚΑΝΟΤΗΤΑ, Δ. ΣΥΣΤΗΜΑΤΑ ΔΙΑΣΦΑΛΙΣΗΣ ΠΟΙΟΤΗΤΑΣ ΚΑΙ ΠΡΟΤΥΠΑ ΠΕΡΙΒΑΛΛΟΝΤΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ), παρακαλούμε όπως επιβεβαιώσετε ότι εν προκειμένω, για την προαπόδειξη της πλήρωσης των κριτηρίων επιλογής των § 2.2.4, 2.2.5, 2.2.6, 2.2.7 της Διακήρυξης, κατά το στάδιο της υποβολής της προσφοράς δια του ΕΕΕΣ, αρκεί μόνη η συμπλήρωση της «Γενικής ένδειξης για όλα τα κριτήρια επιλογής» του μέρους IV του ΕΕΕΣ και δεν απαιτείται η εκ νέου διαμόρφωση και συμπλήρωση των ανωτέρω αναφερόμενων πεδίων του ΕΕΕΣ τόσο από όλους τους συμμετέχοντες οικονομικούς φορείς όσο και από τους παρόχους στήριξης τεχνικής και επαγγελματικής ικανότητας.

Απάντηση:

Βλέπε απάντηση ερωτήματος 31 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 37ο:

Σχετικά με την προδιαγραφή 2.3, της Κατηγορίας Δ.2.2 – FIREWALL, του Πίνακα Συμμόρφωσης (Παράρτημα ΙΙ, σελ.152) παρακαλούμε όπως διευκρινίσετε κατά πόσο η απαίτηση για 25G θύρες έχει περιληφθεί εκ παραδρομής, καθώς το ζητούμενο firewall throughput είναι 17Gbps και κατά συνέπεια δεν προκύπτει τεχνικός λόγος για προσφορά θυρών ταχύτητας 25Gbps.

Απάντηση:

Βλέπε απάντηση ερωτήματος 32 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 38ο:

Σχετικά με την αναφορά σε "VPN Concentrators" (σελ. 97, 102, 105, 164), παρακαλούμε όπως διευκρινίσετε κατά πόσο γίνεται αναφορά στην προσφορά τους εκ παραδρομής, καθότι αφενός δεν βρίσκουμε τεχνικές προδιαγραφές, αφετέρου η λειτουργικότητα ενός VPN Concentrator συνήθως καλύπτεται από το ζητούμενο λογισμικό του πίνακα Δ.2.2 - FIREWALL, απαιτήσεις 4.48 - 4.57.

Απάντηση:

Βλέπε απάντηση ερωτήματος 33 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 39ο:

Σχετικά με την αναφορά στην προσφορά εξοπλισμού "Network Monitoring Tools" (σελ. 97, 102, 105, 164), παρακαλούμε όπως διευκρινίσετε κατά πόσο γίνεται αναφορά στην προσφορά τους εκ παραδρομής, καθότι δεν βρίσκουμε τεχνικές προδιαγραφές στο τεύχος της Διακήρυξης.

Απάντηση:

Βλέπε απάντηση ερωτήματος 34 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 40ο:

Στην §2.2.9.2 Αποδεικτικά μέσα - Δικαιολογητικά προσωρινού αναδόχου, σημείο Β4 «Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6 οι οικονομικοί φορείς προσκομίζουν:» [...] Α1) Αν οι αποδέκτες των υπηρεσιών των έργων είναι φορείς του δημόσιου ή του ευρύτερου δημόσιου τομέα (Αναθέτουσες Αρχές) [...] Επίσης, θα πρέπει να υποβληθούν και τα αντίγραφα των υπογεγραμμένων συμβάσεων των έργων. [...] Εφόσον δεν είναι δυνατή η προσκόμιση των παραπάνω, προσκομίζεται υπεύθυνη δήλωση του οικονομικού φορέα, στην οποία θα αναφέρεται ο λόγος για τον οποίο δεν κατέστη εφικτή η προσκόμιση των παραπάνω δικαιολογητικών και η οποία θα συνοδεύεται *από αντίγραφο του τιμολογίου και, εφόσον υφίσταται, της σχετικής σύμβασης.*».

Παρακαλούμε όπως επιβεβαιώσετε ότι για τα έργα που αφορούν φορείς του δημοσίου ή του ευρύτερου δημοσίου τομέα και δεδομένου ότι οι σχετικές συμβάσεις έχουν ήδη αναρτηθεί και δημοσιοποιηθεί στο Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ) αντί της προσκόμισης αντιγράφων των συμβάσεων, είναι αποδεκτή η αναφορά του μοναδικού αριθμού ΑΔΑΜ κάθε σύμβασης, ως πλήρως και επαρκούς στοιχείου ταυτοποίησης/τεκμηρίωσης της απαίτησης. Επίσης, παρακαλούμε όπως αποσαφηνιστεί αν είναι αποδεκτή και επαρκής τεκμηρίωση, η συνοδεία του Πρωτόκολλου Παραλαβής από Υπεύθυνη Δήλωση του οικονομικού φορέα, στην περίπτωση που από το 1ο δεν συμπεραίνονται σαφώς τα ζητούμενα της §2.2.9.2 Αποδεικτικά μέσα - Δικαιολογητικά προσωρινού αναδόχου, σημείο Β4 (Α1) *«[…] Από τα αναγραφόμενα στα παραπάνω έγγραφα, θα πρέπει να συμπεραίνεται η άρτια και εντός του χρονοδιαγράμματος υλοποίηση του έργου, η ημερομηνία ολοκλήρωσής του, το αντικείμενο της υπηρεσίας, το τελικό καταβληθέν οικονομικό τίμημα.[...]».*

Απάντηση:

Επιβεβαιώνεται, για έργα που αφορούν φορείς του δημόσιου τομέα και των οποίων οι συμβάσεις έχουν αναρτηθεί στο ΚΗΜΔΗΣ, η αναφορά του μοναδικού αριθμού ΑΔΑΜ γίνεται αποδεκτή ως ισοδύναμο αποδεικτικό ταυτοποίησης, εφόσον εξ αυτού συμπεραίνονται άρτια: αντικείμενο, ημερομηνία ολοκλήρωσης και τελικό καταβληθέν τίμημα.

Εφόσον από το Πρωτόκολλο Παραλαβής δεν συμπεραίνονται σαφώς τα ανωτέρω στοιχεία, γίνεται αποδεκτή η συνοδεία του με Υπεύθυνη Δήλωση του οικονομικού φορέα στην οποία αναφέρονται τα ελλείποντα στοιχεία.

Ερώτημα 41ο:

Στην §2.2.9.2 Αποδεικτικά μέσα - Δικαιολογητικά προσωρινού αναδόχου, σημείο Β4 «Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6 οι οικονομικοί φορείς προσκομίζουν:» [...] Α2) Αν ο αποδέκτης είναι ιδιωτικός φορέας, η παροχή θα αποδεικνύεται με βεβαίωση / δήλωση του αποδέκτη ή υπεύθυνη δήλωση του υποψήφιου οικονομικού φορέα, εφόσον δεν είναι δυνατή η προσκόμιση της βεβαίωσης, και την προσκόμιση της σχετικής έγγραφης Σύμβασης (αντίγραφο) (όπου κι εδώ από τα αναγραφόμενα θα πρέπει να συμπεραίνονται τα παραπάνω στοιχεία του σημείου Α).». Δεδομένου ότι:

Α) οι απαιτήσεις τεχνικής ικανότητας της Παρ. 2.2.6.Α της Διακήρυξης περί των έργων δεν απαιτούν κάλυψη συγκεκριμένου προϋπολογισμού ή οικονομικού μεγέθους

Β) οι συμβάσεις στον ιδιωτικό τομέα προστατεύονται, ως επί το πλείστον, από ρήτρες εμπιστευτικότητας

Παρακαλούμε όπως επιβεβαιώσετε ότι, η Αναθέτουσα Αρχή δύναται να αποδεχθεί, αντί της σύμβασης, ένα από τα παρακάτω, τα οποία παρέχουν πλήρη και ελέγξιμη απόδειξη της καλής εκτέλεσης:

- Βεβαίωση καλής εκτέλεσης από τον ιδιώτη πελάτη, από την οποία προκύπτουν τα στοιχεία του έργου και στην οποία δύναται να μην αναφέρεται ο προϋπολογισμός του έργου λόγω εμπιστευτικότητας, ή
- Υπεύθυνη δήλωση του οικονομικού φορέα στην οποία δύναται να μην αναφέρεται ο προϋπολογισμός του έργου λόγω εμπιστευτικότητας, συνοδευόμενη από στοιχεία επικοινωνίας του πελάτη, ώστε η Αναθέτουσα Αρχή να μπορεί να προβεί σε διασταύρωση/επιβεβαίωση

Απάντηση:

Στην περίπτωση συμβάσεων του ιδιωτικού τομέα που προστατεύονται από ρήτρες εμπιστευτικότητας:

Όταν προσκομίζεται βεβαίωση/δήλωση αποδέκτη από την οποία συμπεραίνονται όλα τα απαιτούμενα στοιχεία (αντικείμενο, ημερομηνία ολοκλήρωσης) εκτός του προϋπολογισμού του έργου θα πρέπει παράλληλα να προσκομίζεται βεβαίωση/δήλωση του αποδέκτη με τα στοιχεία επικοινωνίας του και την δέσμευση ότι μπορεί να παρέχει στην Αναθέτουσα Αρχή το ποσό του προϋπολογισμού του έργου αν και όποτε αυτό ζητηθεί.

Όταν προσκομίζεται υπεύθυνη δήλωση του οικονομικού φορέα, χωρίς να προσκομίζεται βεβαίωση/δήλωση αποδέκτη, απαιτούνται επίσης α) αντίγραφο σύμβασης με διαγραμμένα τα ποσά όπου αυτά αναφέρονται και β) βεβαίωση/δήλωση του αποδέκτη με τα στοιχεία επικοινωνίας του και την δέσμευση ότι μπορεί να παρέχει στην Αναθέτουσα Αρχή το ποσό του προϋπολογισμού του έργου αν και όποτε αυτό ζητηθεί.

Ερώτημα 42ο:

Στο ΠΑΡΑΡΤΗΜΑ ΙΙ-ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ της διακήρυξης περιλαμβάνονται και ζητούνται, μεταξύ άλλων, οι ακόλουθες κατηγορίες (λύσεις):

- *Α.1 IDM / IAM / Multi-Factor Authentication (MFA)*
- *Α.3 ENDPOINT SECURITY*

- *A.4 Application microsegmentation*
- A.5 Network Access Control
- A.6 Perimeter / Email Security

Ωστόσο, στο υπόδειγμα της Οικονομικής Προσφοράς δεν εντοπίζεται διακριτή ενότητα ή γραμμή στην οποία να αποτυπώνονται οι ανωτέρω προσφερόμενες λύσεις.
Παρακαλούμε να διευκρινίσετε σε ποια ενότητα της Οικονομικής Προσφοράς θα πρέπει να συμπεριληφθεί το κόστος των ανωτέρω λύσεων, καθώς και εάν αυτό θα πρέπει να αποτυπωθεί διακριτά ή να θεωρηθεί ότι περιλαμβάνεται σε άλλη κατηγορία του υποδείγματος οικονομικής προσφοράς.

- Παρακαλούμε για τις σχετικές οδηγίες προκειμένου να εξασφαλιστεί η ομοιόμορφη και ορθή υποβολή των οικονομικών προσφορών από όλους τους συμμετέχοντες

Απάντηση:

Στο αντικείμενο Α περιλαμβάνονται η προμήθεια αδειών και οι απαραίτητες υπηρεσίες από τον Ανάδοχο για τις προσφερόμενες λύσεις (turn-key solution).

Ερώτημα 43ο:

Στην § 3.1.2.3 Α.3 Endpoint Security, του ΠΑΡΑΡΤΗΜΑΤΟΣ Ι-ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ της διακήρυξης γίνεται η παρακάτω αναφορά:

«Υλοποίηση λύσεων προστασίας τερματικών με χρήση Microsoft Defender for Endpoint. Το σύστημα προστασίας endpoints πρέπει να παρέχει ολοκληρωμένη προστασία για όλα τα endpoints (σταθερά, laptops, VDI, thin clients), να υποστηρίζει real-time protection, behavioral analysis, machine learning και να ενσωματώνεται με τα υπάρχοντα συστήματα Microsoft».

Παρακαλούμε όπως επιβεβαιώσετε εάν η αναφορά στο Microsoft Defender for Endpoint έχει τεθεί εκ παραδρομής ως ενδεικτική αναφορά προϊόντος και ότι η απαίτηση καλύπτεται από οποιαδήποτε προσφερόμενη λύση Endpoint Security, η οποία πληροί τις τεχνικές προδιαγραφές και απαιτήσεις της διακήρυξης, σύμφωνα με το υποβληθέν ΠΑΡΑΡΤΗΜΑ ΙΙ-ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ α/α Α.3. End Point Security και τα χαρακτηριστικά της προσφερόμενης λύσης.

Σε περίπτωση καταφατικής απάντησης, παρακαλούμε όπως επιβεβαιώσετε ότι η υλοποίηση μπορεί να πραγματοποιηθεί με την προσφερόμενη λύση του αναδόχου, εφόσον αυτή καλύπτει πλήρως τις απαιτήσεις της παραγράφου και των πινάκων συμμόρφωσης.

Απάντηση:

Η αναφορά σε Microsoft Defender αφορά την υφιστάμενη εμπειρία και τεχνογνωσία καθώς και τις τεχνολογικές υποδομές του Φορέα, και δεν αποκλείει ισοδύναμες πλατφόρμες άλλων κατασκευαστών, εφόσον καλύπτουν πλήρως τις προδιαγραφές του Πίνακα Συμμόρφωσης, τεκμηριώνεται η πλήρης λειτουργική ισοδυναμία και διασφαλίζεται ενοποίηση με το περιβάλλον του φορέα.

Ερώτημα 44ο:

Σε περίπτωση που η Υλοποίηση λύσεων προστασίας τερματικών (όπως αναφέρεται στην § 3.1.2.3 Α.3 Endpoint Security, του ΠΑΡΑΡΤΗΜΑΤΟΣ Ι-ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ) είναι με χρήση Microsoft Defender for Endpoint παρακαλούμε όπως διευκρινιστεί ότι οι απαιτούμενες άδειες Microsoft Defender for Endpoint θα διατεθούν από την αναθέτουσα.

Απάντηση:

Ο φορέας διαθέτει ήδη άδειες Ε3 μέσω του enterprise agreement της ΓΓΠΣΔΔ οι οποίες αναμένεται να επεκταθούν/μετατραπούν σε Ε5 (μέσω του enterprise agreement της ΓΓΠΣΔΔ).

Ερώτημα 45ο:

Στις απαιτήσεις της πλατφόρμας Enterprise Ready Penetration Testing Framework, περιλαμβάνεται δυνατότητα Wireless Penetration Testing. Καθώς η απαίτηση αφορά σε:

- Διαφορετικό αντικείμενο και τεχνολογικό τομέα

Το Wireless Penetration Testing αποτελεί εξειδικευμένο πεδίο αξιολόγησης ασφάλειας ασύρματων δικτύων (Wi-Fi), το οποίο βασίζεται σε εξειδικευμένο εξοπλισμό (wireless adapters, antennas, packet injection capabilities κ.λπ.) και εξειδικευμένα εργαλεία ανάλυσης πρωτοκόλλων 802.11. Αντίθετα, οι enterprise πλατφόρμες Penetration Testing Frameworks εστιάζουν κυρίως σε αξιολογήσεις εφαρμογών, υποδομών, δικτύων, Active Directory, cloud περιβαλλόντων και αυτοματοποίηση διαδικασιών ελέγχου ασφαλείας.

- Μη συνήθη απαίτηση σε Enterprise Penetration Testing Frameworks

Η δυνατότητα Wireless Penetration Testing δεν αποτελεί τυπικό ή βασικό χαρακτηριστικό των περισσότερων εμπορικών enterprise-ready penetration testing frameworks. Συνήθως υλοποιείται μέσω εξειδικευμένων εργαλείων και συσκευών που λειτουργούν συμπληρωματικά και όχι ως εγγενές χαρακτηριστικό της κεντρικής πλατφόρμας.

Παρακαλούμε όπως επιβεβαιώσετε ότι η απαίτηση Wireless Penetration Testing έχει συμπεριληφθεί εκ παραδρομής και όπως διευκρινίσετε ότι η κάλυψή της δεν αποτελεί υποχρεωτικό κριτήριο συμμόρφωσης για την προσφερόμενη Enterprise Ready Penetration Testing Framework πλατφόρμα.

Απάντηση:

Η απαίτηση για Wireless Penetration Testing θεωρείται απαραίτητη για την προστασία των Wireless δικτύων του Φορέα και δεν εχει περιληφθεί εκ παραδρομής. Η δυνατότητα Wireless Penetration Testing δεν είναι υποχρεωτικό να αποτελεί ενσωματωμένη λειτουργικότητα του Enterprise Ready Penetration Testing Framework, αλλά δύναται να υλοποιείται μέσω εξειδικευμένων εργαλείων/εξοπλισμού που συμπληρώνουν την κεντρική πλατφόρμα, χωρίς να αποτελεί εγγενές χαρακτηριστικό της.

Ερώτημα 46ο:

Παρακαλούμε όπως επιβεβαιώσετε πως υφίστανται διαθέσιμες από την Αναθέτουσα Αρχή οι αναγκαίες λύσεις και άδειες λογισμικού για την κάλυψη των απαιτήσεων που γίνονται αναφορά στο ΠΑΡΑΡΤΗΜΑ Ι-παράγραφος 3.1.2.2. Α.2 προστασία Δεδομένων ,και συγκεκριμένα για τα:

- Database Protection για Oracle 19c (π.χ. Oracle Advanced Security, Database Vault, Audit Vault & Database Firewall),
- Data-at-Rest Encryption AES-256 σε storage, βάσεις (Oracle TDE), file servers και backups, καθώς και Data-in-Transit Encryption (TLS 1.2/1.3),
- Key Management μέσω HSM ή cloud key management (Azure Key Vault / Oracle Key Vault),

και ότι δεν απαιτείται η προμήθεια των εν λόγω λύσεων και αδειών από τον Ανάδοχο.

Απάντηση:

Βλέπε απάντηση ερωτήματος 34 πρώτου τεύχους ερωτήσεων απαντήσεων.

Ερώτημα 47ο:

Λαμβάνοντας υπόψη την ιδιαίτερη πολυπλοκότητα και το εύρος του υπό ανάθεση έργου, καθώς και τον σημαντικό όγκο τεχνικών απαιτήσεων που πρέπει να αναλυθούν και να τεκμηριωθούν με ακρίβεια, παρακαλούμε όπως εξετάσετε τη χορήγηση παράτασης της προθεσμίας υποβολής προσφορών κατά δέκα (10) ημερολογιακές ημέρες. Η εν λόγω παράταση θα επιτρέψει την ολοκληρωμένη μελέτη όλων των παραμέτρων του έργου και τη σύνταξη μιας άρτιας, πλήρως τεκμηριωμένης και ανταγωνιστικής τεχνικής και οικονομικής προσφοράς, η οποία θα ανταποκρίνεται με τον βέλτιστο τρόπο στις απαιτήσεις της Διακήρυξης και στις ανάγκες της Αναθέτουσας Αρχής.

Απάντηση:

Το αίτημα παράτασης έχει ληφθεί υπόψη.

Ερώτημα 48ο:

Στο πλαίσιο της ως άνω Διακήρυξης και με σκοπό την υποβολή ολοκληρωμένης και ορθά κοστολογημένης προσφοράς, υποβάλλουμε εγκαίρως τα κάτωθι διευκρινιστικά ερωτήματα. Τα ερωτήματα αφορούν ασάφειες ως προς το μέγεθος του πληθυσμού χρηστών/συστημάτων και ως προς το ακριβές εύρος των ζητούμενων προϊόντων και υπηρεσιών. Παρακαλούμε για τις διευκρινίσεις σας.

Α. Πίνακας Δ.1 — «Λογισμικό Ασφάλειας»

Α/Α	**Σημείο Διακήρυξης**	**Διευκρινιστικό Ερώτημα**
Α.1	Πίνακας Δ.1 — SIEM (Έτος 3)	Παρακαλούμε διευκρινίστε εάν το Έτος 3 αφορά αποκλειστικά συντήρηση/υποστήριξη με διατήρηση της κάλυψης του Έτους 2 (2.000

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
		endpoints / 15TB logs) ή εάν προβλέπεται περαιτέρω επέκταση. Είναι η επέκταση +500 endpoints / +5TB του Έτους 2 σωρευτική και διατηρούμενη καθ' όλη τη διάρκεια; **Απάντηση**: Η επέκταση των +500 endpoints / +5TB είναι σωρευτική και διατηρούμενη καθ'όλη τη διάρκεια.
Α.2	Πίνακας Δ.1 — Βάση μεγέθους (endpoints vs χρήστες)	Το SIEM προσδιορίζεται σε endpoints (1.500), ενώ ο Πίνακας Β.1 αναφέρει 1.900 χρήστες. Παρακαλούμε διευκρινίστε τη σχέση των δύο μεγεθών και ποιο αποτελεί την επίσημη βάση αδειοδότησης για τα προϊόντα που τιμολογούνται ανά χρήστη/endpoint. Από τους πίνακες συμμόρφωσης προκύπτει ζήτηση για τουλάχιστον 2.700 χρήστες του οργανισμού. **Απάντηση** Η τελική (Year 3) ανάγκη θα είναι για κάλυψη τουλάχιστον 2.700 χρηστών, όπως αναφέρεται και στην Παράγραφο 3.1.1 – Υφιστάμενη Κατάσταση.
Α.3	Πίνακας Δ.1 — WAF	Για το WAF, παρακαλούμε διευκρινίστε σε ποιο έτος αντιστοιχεί η εργασία «Συντήρηση / tuning» και εάν το «+1 B2B interface» του Έτους 2 διατηρείται στο Έτος 3. Επιβεβαιώστε ότι η απαίτηση «Πλήρης προστασία APIs» καλύπτει το σύνολο των 4 περιβαλλόντων (prod/test/train/parallel) πλέον του B2B interface. **Απάντηση** Η συντήρηση / tuning αφορά και τα τρία έτη, αλλά στο έτος 3 είναι η μοναδική προβλεπόμενη ανάγκη. Η Πλήρης προστασία APIs καλύπτει όντως το σύνολο των 4 περιβαλλόντων.
Α.4	Πίνακας Δ.1 — DSR Tools	Τα DSR Tools προσδιορίζονται ως «1 instance». Παρακαλούμε διευκρινίστε τον εκτιμώμενο ετήσιο όγκο αιτημάτων υποκειμένων (DSR volume) και τον αριθμό χρηστών διαχείρισης (administrators/agents), ώστε να καταστεί δυνατή η ορθή διαστασιολόγηση και αδειοδότηση. Υπάρχουν άλλες προδιαγραφές ή μπορούν να προσφερθούν και open source εργαλεία?

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
		Απάντηση Λοιπές τεχνικές λεπτομέρειες και στοιχεία θα παρασχεθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης. Γίνονται αποδεκτές τόσο commercial όσο και open source λύσεις, εφόσον πληρούν τις λειτουργικές απαιτήσεις.
Α.5	Πίνακας Δ.1 — Εργαλεία «Enterprise license»	Για τα Vulnerability Scanning Tools, Penetration Testing Frameworks, Compliance Management Platform, Threat Intelligence Platform και Training platform δίνεται μόνο η ένδειξη «Enterprise license», χωρίς ποσότητες ανά έτος (στήλες κενές). Παρακαλούμε διευκρινίστε ανά εργαλείο: (α) το εύρος (αριθμός assets / IPs / scans / χρηστών), (β) το μοντέλο αδειοδότησης (perpetual, subscription ή SaaS), (γ) τη διάρκεια κάλυψης και τη συντήρηση/υποστήριξη ανά έτος (Έτη 1–3). Υπάρχουν άλλες προδιαγραφές ή μπορούν να προσφερθούν και open source εργαλεία? **Απάντηση** Λοιπές τεχνικές λεπτομέρειες και στοιχεία θα παρασχεθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης. Γίνονται αποδεκτές τόσο commercial όσο και open source λύσεις, εφόσον πληρούν τις λειτουργικές απαιτήσεις.
Α.6	Πίνακας Δ.1 — Training platform	Για το «Training platform» δεν αναφέρεται αριθμός χρηστών/αδειών ούτε παρατηρήσεις. Παρακαλούμε διευκρινίστε τον αριθμό αδειοδοτούμενων χρηστών (π.χ. 1.900) και εάν η πλατφόρμα ταυτίζεται με την «E-learning Platform» του Πίνακα Β.1.3 (βλ. ερώτημα Γ.3). Επειδή δεν υπάρχουν προδιαγραφές η πλατφόρμα θα καλύπτει ασύγχρονη εκπαίδευση ή /και σύγχρονη. Υπάρχουν άλλες προδιαγραφές ή μπορούν να προσφερθούν και open source εργαλεία? **Απάντηση** Η πλατφόρμα θα πρέπει να καλύπτει τουλάχιστον ασύγχρονη εκπαίδευση. Η αδειοδότηση θα πρέπει να καλύπτει 3.000 χρήστες. Οι λοιπές τεχνικές προδιαγραφές θα πρέπει να προταθούν τεκμηριωμένα από τον Ανάδοχο στην τεχνική

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
		προσφορά. Γίνονται αποδεκτές τόσο commercial όσο και open source λύσεις, εφόσον πληρούν τις λειτουργικές απαιτήσεις.

Β. Ενότητα 1.1.1.3 — «Εξειδικευμένα Εργαλεία»

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
Β.1	§1.1.1.3 — Database security tools	Αναφέρεται «Oracle Audit Vault». Παρακαλούμε διευκρινίστε εάν γίνονται αποδεκτές ισοδύναμες/εναλλακτικές λύσεις ή εάν πρόκειται για αποκλειστική απαίτηση. Παρακαλούμε επίσης γνωστοποιήστε τον αριθμό των Oracle 19c instances προς κάλυψη, ώστε να είναι εφικτή η διαστασιολόγηση. **Απάντηση** Βλέπε απάντηση ερωτήματος 23 πρώτου τεύχους.
Β.2	§1.1.1.3 — Backup & DR software	Ζητούνται «RPO/RTO targets» και «3-2-1 backup strategy» χωρίς αριθμητικές τιμές. Παρακαλούμε προσδιορίστε τις στοχευόμενες τιμές RPO/RTO, τον συνολικό όγκο δεδομένων προς προστασία και τον αριθμό/τύπο των συστημάτων που εμπίπτουν στο εύρος. Απαιτείται να προσφερθεί σχετική πλατφόρμα Backup? **Απάντηση** Στόχοι RPO/RTO: ≤ 4 ώρες (§3.1.3.9). Απαιτείται προσφορά πλατφόρμας Backup & DR software ως παραδοτέο. Λοιπές τεχνικές λεπτομέρειες και στοιχεία θα παρασχεθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.
Β.3	§1.1.1.3 — Penetration Testing Frameworks	Παρακαλούμε διευκρινίστε εάν ζητείται προϊόν/πλατφόρμα (framework) υπό «Enterprise license» ή η παροχή υπηρεσιών διενέργειας penetration testing (assessments). Σε περίπτωση υπηρεσίας, προσδιορίστε τη συχνότητα/πλήθος assessments ανά έτος και το εύρος (web/network/wireless/social engineering). **Απάντηση** Ζητείται πλατφόρμα/εργαλείο (framework) υπό Enterprise license (Δ.1.5) και παροχή υπηρεσιών pentest (Β.2.7). Είναι δύο διακριτά αντικείμενα. Το

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
		πλήθος των Δοκιμών Ασφαλείας (Penetration testing) που δυνητικά (ad-hoc υλοποιήσεις) θα διενεργηθούν συνολικά κατά την διάρκεια του έργου φαίνεται στον πίνακα Πίνακα Β.2.7 της Οικονομικής προσφοράς (η τιμολόγηση γίνεται ανά άσκηση). Εύρος: web applications, network infrastructure, Active Directory, cloud, wireless (εφόσον εφαρμόζεται).
Β.4	§1.1.1.3 & Πίνακας Δ.1 — Επικαλύψεις	Οι κατηγορίες Vulnerability Scanning, Penetration Testing, Compliance Management και Threat Intelligence εμφανίζονται τόσο στον Πίνακα Δ.1 όσο και στην §1.1.1.3. Παρακαλούμε διευκρινίστε εάν πρόκειται για το ίδιο αντικείμενο (περιγραφόμενο σε δύο σημεία) ή για διακριτές απαιτήσεις, προς αποφυγή διπλής τιμολόγησης. **Απάντηση** Τα εργαλεία Vulnerability Scanning, Penetration Testing, Compliance Management, Threat Intelligence εμφανίζονται στο ίδιο αντικείμενο - περιγράφονται στη §3.1.5.3 και τιμολογούνται στον Πίνακα Δ.1. Δεν πρόκειται για διακριτές απαιτήσεις. Στην οικονομική προσφορά αναφέρεται μία γραμμή στον Πίνακα Δ.1 ανά εργαλείο.
Β.5	§1.1.1.3 — Συμμόρφωση / GDPR / DSR	Οι λειτουργίες «Compliance Management Platform» (ISO 27001/GDPR/NIS2), «GDPR compliance tools (DSR management)» και «DSR Tools» (Πίνακας Δ.1) εμφανίζουν επικάλυψη. Παρακαλούμε διευκρινίστε εάν απαιτείται ενιαία ολοκληρωμένη πλατφόρμα ή διακριτά προϊόντα ανά λειτουργία. **Απάντηση** Τα εν λόγω εργαλεία μπορούν να παρέχονται ως ενιαία ολοκληρωμένη πλατφόρμα ή ως διακριτά προϊόντα. Η διακήρυξη δεν επιβάλλει συγκεκριμένη αρχιτεκτονική. Ο Ανάδοχος τεκμηριώνει πώς καλύπτεται η κάθε λειτουργία. Εφόσον πλέον του ενός αντικειμένου του Πίνακα Δ.1 καλύπτεται από μια ενιαία ολοκληρωμένη πλατφόρμα, ο Ανάδοχος καλείται να κατανείμει (κατά προσέγγιση) το συνολικό κόστος της ενιαίας πλατφόρμας ανά γραμμή του Πίνακα Δ.1.

Γ. Πίνακας Β.1 — «Εφάπαξ Παροχή Υπηρεσιών»

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
Γ.1	Πίνακας Β.1.3 — Μέγεθος πληθυσμού	Το Security Awareness Program αναφέρεται σε 1.900 χρήστες, ενώ ο Πίνακας Δ.1 χρησιμοποιεί 1.500 endpoints. Παρακαλούμε επιβεβαιώστε το επίσημο μέγεθος (named users / endpoints) που πρέπει να ληφθεί υπόψη για τη διαστασιολόγηση των υπηρεσιών και των per-user προϊόντων. **Απάντηση** Βλέπε απάντηση ερωτήματος 48 (Α.6)
Γ.2	Πίνακας Β.1.3 — Specialized Training & Knowledge Transfer	Παρακαλούμε προσδιορίστε τον αριθμό και τις ομάδες/ρόλους αποδεκτών για το «Specialized Training» και το «Knowledge Transfer» (π.χ. ομάδα IT/Security, διοίκηση), καθώς και τον προβλεπόμενο αριθμό συνεδριών/ωρών. **Απάντηση** Κατά κανόνα, η εξειδικευμένη εκπαίδευση (Specialized Training) απευθύνεται σε στελέχη IT/Security, στελέχη διοίκησης και χρήστες υψηλού κινδύνου. Οι ομάδες χρηστών καθώς και οι προβλεπόμενες συνεδρίες και η διάρκεια αυτών σε ώρες θα προσδιοριστούν στο πλαίσιο Μελέτης Εφαρμογής.
Γ.3	Πίνακας Δ.1 & Β.1.3 — Πλατφόρμα εκπαίδευσης	Παρακαλούμε διευκρινίστε τη σχέση μεταξύ του «Training platform» (Πίνακας Δ.1 — προϊόν/άδεια) και της «E-learning Platform» (Πίνακας Β.1.3 — παραδοτέο υπηρεσίας): πρόκειται για το ίδιο αντικείμενο ή για δύο διακριτές απαιτήσεις; **Απάντηση** Η «Training Platform» (Δ.1.8) είναι η πλατφόρμα/άδεια (κόστος Μέρους Δ), ενώ η «E-learning Platform» της Β.1.3 αφορά την υπηρεσία δημιουργίας περιεχομένου και παροχής εκπαίδευσης (μέρος του κόστους των υπηρεσιών της Β.1.3). Δεν αποτελούν διακριτές απαιτήσεις αλλά δύο διαστάσεις (λογισμικό + υπηρεσία) του ίδιου αντικειμένου. Διευκρινίζεται ότι η παράγραφος Β.1.3 περιλαμβάνει και επιπλέον υπηρεσίες της e-Learning platform, η πλατφόρμα e-Learning χρησιμοποιείται, όπου αυτή απαιτείται, για την παροχή των υπηρεσιών της Β.1.3.
Γ.4	Παρ.3.1.3.3 Training & Awareness «…Δημιουργία	Παρακαλούμε διευκρινίστε την ποσότητα του εκπαιδευτικού υλικού και το πλήθος των εκπαιδεύσεων σε ποιες κατηγορίες ομάδων

Α/Α	Σημείο Διακήρυξης	Διευκρινιστικό Ερώτημα
	εκπαιδευτικού υλικού και διεξαγωγή εκπαιδεύσεων σε στοχευμένες ομάδες Το εκπαιδευτικό υλικό πρέπει να είναι customized για τους ειδικούς ρόλους του Κτηματολογίου, να περιλαμβάνει interactive scenarios, να είναι διαθέσιμο σε ελληνική γλώσσα και να περιλαμβάνει compliance-specific modules για GDPR, NIS2 και ISO 27001.»	απευθύνονται και πόσες ώρες περιλαμβάνουν. **Απάντηση** Το εκπαιδευτικό υλικό απευθύνεται σε στελέχη IT/Security, στελέχη διοίκησης και χρήστες υψηλού κινδύνου. Οι ομάδες χρηστών καθώς και οι προβλεπόμενες συνεδρίες θα προσδιοριστούν στο πλαίσιο Μελέτης Εφαρμογής. Το υλικό θα είναι στην ελληνική γλώσσα, προσαρμοσμένο για τους ρόλους του Κτηματολογίου, και θα περιλαμβάνει τμήματα για GDPR, NIS2 και ISO 27001. Τα ανωτέρω θα προσδιοριστούν στη Μελέτη Εφαρμογής..

Ερώτημα 49ο:

Στο Κεφάλαιο 3.1.3.10.Β.2.7 Δοκιμές Ασφάλειας (Penetration testing), επιθυμούμε να διευκρινιστεί/ αναφερθεί:

Αριθμός web/ mobile apps και το μέγεθός τους

Αριθμός external IPs/ Domains για το external penetration test

Αριθμός internal machine for VA

Αριθμός internal domain για internal penetration test

Απάντηση:

Περαιτέρω προδιαγραφές και λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 50ο:

Στο Κεφάλαιο 3.1.3.10.Β.2.8 Red team exercises, επιθυμούμε να διευκρινιστεί/ αναφερθεί αν το Red Teaming exercise πρόκειται να Cyber & Physical και Physical σε πόσα σημεία.

Απάντηση:

Το αντικείμενο αφορά Cyber Red Team (full-scope adversary simulation κατά της ψηφιακής υποδομής, Active Directory, cloud environments, applications). Το physical component (π.χ. physical intrusion testing, social engineering on-site, badge cloning) δεν αποτελεί υποχρεωτική απαίτηση του Β.2.8 και δεν αναφέρεται στις τεχνικές προδιαγραφές.

Ερώτημα 51ο:

Υφιστάμενη Υποδομή & Asset Inventory

Υπάρχει διαθέσιμη αναλυτική απογραφή της υφιστάμενης υποδομής (ενδεικτικά: πλήθος endpoints, servers, applications, databases και χρηστών ανά κατηγορία);

Υπάρχει διαθέσιμη κατηγοριοποίηση των κρίσιμων συστημάτων (critical/ non- critical);

Απάντηση:

Βλέπε απάντηση ερωτήματος 45 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 52ο:

Υφιστάμενα Συστήματα Ασφαλείας & Ενοποιήσεις

Ποια συστήματα ασφαλείας λειτουργούν σήμερα (π.χ. SIEM, IAM, EDR/ XDR, DLP κ.λπ.);

Απαιτείται πλήρης αντικατάσταση των υφιστάμενων λύσεων ή ενσωμάτωση τους (intergration);

Υπάρχουν συγκεκριμένες απαιτήσεις για διατήρηση legacy συστημάτων;

Απάντηση:

Συνοπτικά: υπάρχει εγκατεστημένη υποδομή και διατάξεις ασφαλείας (SOC/QRADAR, NGFW, WAF) στα primary datacenters του φορέα. Η σύμβαση με την οποία καλύπτεται η λειτουργία λήγει τον Νοέμβριο 2026. Ο προγραμματισμός και το χρονοδιάγραμμα μετάβασης από την υπάρχουσα υποδομή σε τυχόν νέα θα πρέπει συμπεριλαμβάνεται στην τεχνική προσφορά του αναδόχου.

Ερώτημα 53ο:

Λειτουργία SOC & Υπηρεσιών Παρακολούθησης

Υπάρχει ήδη υφιστάμενο Security Operations Center (SOC) ή απαιτείται πλήρης υλοποίηση εξ αρχής;

Τα 10TB logs που αναφέρονται αφορούν σε ετήσια ή μηνιαία χρήση του SIEM;

Ποιο είναι το retention policy που απαιτείται από τον οργανισμό;

Απάντηση:

Συνοπτικά: υπάρχει εγκατεστημένη υποδομή και διατάξεις ασφαλείας (SOC/QRADAR, NGFW, WAF) στα primary datacenters του φορέα. Η σύμβαση με την οποία καλύπτεται η λειτουργία λήγει τον Νοέμβριο 2026. Ο προγραμματισμός και το χρονοδιάγραμμα μετάβασης από την υπάρχουσα υποδομή σε τυχόν νέα θα πρέπει συμπεριλαμβάνεται στην τεχνική προσφορά του αναδόχου.

Τα 10TB αφορούν ετήσιο συνολικό όγκο ingest (annual ingestion volume) για το Έτος 1, με βάση 1.500 endpoints. Δεν αφορούν μηνιαίο μέγεθος.

Η Διακήρυξη δεν ορίζει ρητά retention policy. Θα καθοριστεί βάσει απαιτήσεων NIS 2 και βέλτιστων πρακτικών για φορείς του Δημοσίου την οποία θα προτείνει ο ανάδοχος στη Μελέτη Εφαρμογής.

Ερώτημα 54ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο: 1.1:

Η προσφερόμενη υπηρεσία να έχει υλοποιηθεί σε οργανισμούς με αντίστοιχο μέγεθος με αυτό του κτηματολόγιο.

Η απαίτηση όπως η προσφερόμενη υπηρεσία να έχει υλοποιηθεί σε οργανισμούς αντίστοιχου μεγέθους με το Κτηματολόγιο περιορίζει σημαντικά τη δυνατότητα συμμετοχής οικονομικών φορέων που διαθέτουν αποδεδειγμένη εμπειρία και τεχνογνωσία σε συναφή έργα. Παρακαλείται να διευκρινιστεί εάν η εν λόγω απαίτηση δύναται να αναδιατυπωθεί ώστε να βασίζεται σε γενικότερα και αντικειμενικά κριτήρια εμπειρίας. Προτείνεται η αντικατάσταση της απαίτησης με κριτήρια όπως ο συνολικός αριθμός επιτυχώς ολοκληρωμένων έργων, η εμπειρία σε συναφείς τομείς ή/και κλάδους, καθώς και η πολυπλοκότητα και το εύρος των υλοποιήσεων, ώστε να διασφαλίζεται η αναλογικότητα και η ενίσχυση του ανταγωνισμού.

Απάντηση:

Η παροχή στοιχείων εκ μέρους του αναδόχου για την απόδειξη των απαιτήσεων και των προδιαγραφών του διαγωνισμού αποτελεί μέρος της τεχνικής προσφοράς του αναδόχου. Η απαίτηση του Πίνακα Συμμόρφωσης, σημείο 1.1, αποτελεί μέρος της Τεχνικής Προσφοράς του Αναδόχου, ο οποίος καλείται να αποδείξει εμπειρία σε περιβάλλοντα αντίστοιχου μεγέθους. Η αξιολόγηση της συμμόρφωσης γίνεται βάσει των στοιχείων που ο Ανάδοχος θα παράσχει (π.χ. αριθμός χρηστών/endpoints, γεωγραφική διασπορά, πολυπλοκότητα υποδομής). Δεν τίθεται αριθμητικό κατώφλι μεγέθους - ο Ανάδοχος αιτιολογεί τη συγκρισιμότητα. Η απαίτηση δεν τροποποιείται

Ερώτημα 55ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο 1.4:

Ο Πάροχος των υπηρεσιών θα πρέπει να έχει εκτενή εμπειρία σε περιβάλλοντα SIEM. Κατ' ελάχιστο να υποστηρίζει Microsoft Sentinel και IBM QRadar SIEM.

Σημείο 8.1:

Η λύση θα πρέπει να ενσωματώνεται με λύσεις SIEM, τουλάχιστον με SPLUNK ή QRADAR

Σημείο 34:

Δυνατότητα integration με λύσεις Security Information and Event Management (SIEM) και ειδικότερα Lancope, Arcsight, RSA, Splunk.

Η απαίτηση για υποστήριξη των Microsoft Sentinel, IBM QRadar SIEM, Splunk, Lanscope, Arcsight, RSA εισάγει αναφορά σε συγκεκριμένους κατασκευαστές και ενδέχεται να περιορίζει τον ανταγωνισμό και πιθανό να αποκλείει ισοδύναμες τεχνολογικές λύσεις. Προτείνεται η διατύπωση των απαιτήσεων σε γενικότερο επίπεδο λειτουργικών δυνατοτήτων SIEM, επιτρέποντας τη συμμετοχή ισοδύναμων λύσεων.

Απάντηση:

Βλέπε απάντηση ερωτήματος 53 Α τεύχους ερωτήσεων/ απαντήσεων.

Ερώτημα 56ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο 2.4:

Ενημέρωση για πιθανά περιστατικά ασφαλείας μέσω:

* Τηλεφωνικής κλήσης,

* email

* SMS

* Collaboration software π.χ. Teams.

Η απαίτηση προτείνεται να τροποποιηθεί ως εξής:

Ενημέρωση για πιθανά περιστατικά ασφαλείας μέσω:

* Τηλεφωνικής κλήσης,

* email

* SMS

* Collaboration software π.χ. Teams ή/και ειδοποιήσεων μέσω mobile εφαρμογής που παρέχεται από τον Ανάδοχο

* Web Portal

Απάντηση:

Τα απαιτούμενα μέσα ενημέρωσης (τηλεφωνική κλήση, email, SMS, collaboration software π.χ. Teams) αποτελούν ελάχιστη απαίτηση του σημείου 2.4. Ο Ανάδοχος υποχρεούται να τα καλύπτει πλήρως. Πρόσθετα μέσα ενημέρωσης (mobile εφαρμογή Αναδόχου, Web Portal) γίνονται αποδεκτά ως συμπληρωματικά. Η τροποποίηση του σημείου 2.4 δεν κρίνεται απαραίτητη.

Ερώτημα 57ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημεία 3.1, 3.3, 3.4, 3.6, 3.7, 3.8 και 3.9:

3.1 Ο Ανάδοχος θα πρέπει να παρέχει υπηρεσία διερεύνησης μέσω τεχνητής νοημοσύνης με χρήση agents (AI agentic).

3.3 Η υπηρεσία να υποστηρίζει πολλαπλούς agents (multi-agent system).

3.4 Να υποστηρίζονται κατ' ελάχιστο οι ακόλουθοι agents:

* Virtual SOC L1 Analyst

* Runbook Agent

* Investigation Agent

* Remediation Agent

* Case Management Agent

3.6 Να υποστηρίζονται κατ' ελάχιστο τα ακόλουθα μοντέλα LLM:

* GPT-4o,

* GPT-4 Turbo,

* Gemini 1 Pro / 1.5 Pro

3.7 Να υποστηρίζονται κατ' ελάχιστο οι ακόλουθες τεχνολογίες:

* Retrieval-Augmented Generation (RAG)

* Model-Context Protocol (MCP)

3.8 Να υποστηρίζεται η αυτοματοποίηση των ροών με χρήση των agents και drag and drop.

3.9 Ο Ανάδοχος θα πρέπει να σχεδιάσει και να υλοποιήσει τις κατάλληλες ροές με χρήση των agents.

Οι απαιτήσεις για συγκεκριμένη αρχιτεκτονική τεχνητής νοημοσύνης (agentic / multi-agent), προκαθορισμένους τύπους agents, συγκεκριμένα LLM μοντέλα όπως GPT-4o, GPT-4 Turbo και Gemini 1.5 Pro, καθώς και τεχνολογίες όπως Retrieval-Augmented Generation και Model Context Protocol, συνιστούν ιδιαίτερα περιοριστική και κατευθυντική προσέγγιση που ενδέχεται να φωτογραφίζει συγκεκριμένες λύσεις. Παρακαλείται να διευκρινιστεί εάν οι εν λόγω απαιτήσεις δύνανται να απαλειφθούν ή να αναδιατυπωθούν. Προτείνεται η αντικατάστασή τους με γενική απαίτηση αξιοποίησης δυνατοτήτων τεχνητής νοημοσύνης για αυτοματοποιημένη διερεύνηση συμβάντων, συμπεριλαμβανομένης της συσχέτισης και ανάλυσης ειδοποιήσεων, της χαρτογράφησης σε τακτικές και τεχνικές του MITRE ATT&CK, της πρότασης ενεργειών απόκρισης και αποκατάστασης, καθώς και της παραγωγής αναφορών.

Απάντηση:

Οι απαιτήσεις των σημείων 3.1–3.9 του Πίνακα Συμμόρφωσης Δ.1.1 (SOAR/AI) περιγράφουν λειτουργικά αποτελέσματα που επιτυγχάνονται μέσω σύγχρονων τεχνολογιών τεχνητής νοημοσύνης. Οι αναφορές σε GPT-4o, GPT-4 Turbo, Gemini 1 Pro/1.5 Pro χρησιμοποιούνται ως ενδεικτικές αναφορές της γενεάς LLM που απαιτείται, όχι ως αποκλειστικά προϊόντα.

Γίνονται αποδεκτές ισοδύναμες λύσεις, εφόσον:

- Παρέχουν AI-powered automated investigation με multi-agent αρχιτεκτονική ισοδύναμης λειτουργικότητας (Virtual SOC Analyst, Runbook automation, Investigation, Remediation)
- Αξιοποιούν LLM γενεάς αντίστοιχης με GPT-4o/Gemini 1.5 Pro ή νεότερης (δεν απαιτείται ο συγκεκριμένος κατασκευαστής)
- Υλοποιούν context-aware investigation μέσω RAG ή ισοδύναμης τεχνολογίας ανάκτησης πληροφορίας
- Υποστηρίζουν tool integration (MCP ή ισοδύναμο πρωτόκολλο)
- Παρέχουν drag-and-drop workflow automation ή αντίστοιχο low-code orchestration

Ο Ανάδοχος τεκμηριώνει στον Πίνακα Συμμόρφωσης τη λειτουργική ισοδυναμία για κάθε σημείο 3.1–3.9.

Ερώτημα 58ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο 4.7:

Αναφορές συμμόρφωσης: Η υπηρεσία να παρέχει τη δυνατότητα αναφοράς ως προς τη συμμόρφωση με κοινώς αποδεκτά πρότυπα στο χώρο της ασφάλειας (ISO 27002, NIST), τα

οποία αντιστοιχίζονται απευθείας σε οποιοδήποτε κανονιστικό πρότυπο ή πολιτική ασφάλειας.

Η απαίτηση για αναφορές συμμόρφωσης βάσει συγκεκριμένων προτύπων όπως ISO/IEC 27002 και NIST ενδέχεται να περιορίζει την αναγνώριση ισοδύναμων πλαισίων και πιστοποιήσεων. Παρακαλείται να διευκρινιστεί εάν η απαίτηση μπορεί να καλυφθεί και μέσω άλλων διεθνώς αναγνωρισμένων προτύπων και πιστοποιήσεων. Προτείνεται η αναδιατύπωση της απαίτησης ώστε να επιτρέπεται η παροχή αναφορών συμμόρφωσης βάσει ισοδύναμων προτύπων, όπως ISO/IEC 27001, ISO 22301 ή SOC 2 Type II, διασφαλίζοντας ευελιξία και ενίσχυση του ανταγωνισμού.

Απάντηση:

Γίνεται αποδεκτή η παροχή αναφορών συμμόρφωσης βάσει ισοδύναμων διεθνώς αναγνωρισμένων πλαισίων, αν και μόνο αν αυτά αντιστοιχίζονται στις απαιτήσεις ISO/IEC 27002 ή NIST CSF. Για παράδειγμα:

- ISO/IEC 27001:2022: Γίνεται αποδεκτό ως ισοδύναμο (controls mapping με ISO 27002).
- NIST CSF 2.0: Γίνεται αποδεκτό ως ισοδύναμο του NIST

Εφόσον η τεχνική λύση δεν χρησιμοποιεί τα ISO 27002, NIST, ο ανάδοχος οφείλει να αποδείξει την δυνατότητα της απόλυτης αντιστοίχισης (mapping).

Ερώτημα 59ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο 4.10:

Δυνατότητα επέκτασης των αναφορών με εργαλεία τεχνητής νοημοσύνης. Να περιγραφεί αναλυτικά.

Η απαίτηση για δυνατότητα επέκτασης των αναφορών με εργαλεία τεχνητής νοημοσύνης, στο πλαίσιο παραγωγής τόσο τεχνικών όσο και διοικητικών αναφορών, δεν προσδιορίζει επαρκώς το αναμενόμενο εύρος λειτουργικότητας. Παρακαλείται να διευκρινιστεί εάν η παροχή αναφορών εμπλουτισμένων με AI-generated insights που σχετίζονται με συμβάντα ασφάλειας (π.χ. ανάλυση, συσχέτιση, προτεινόμενες ενέργειες, συνοπτικά συμπεράσματα για διοίκηση) καλύπτει την εν λόγω απαίτηση.

Απάντηση:

Η δυνατότητα επέκτασης των αναφορών με εργαλεία τεχνητής νοημοσύνης αποτελεί μέρος της τεχνικής προσφοράς του αναδόχου. Συγκεκριμένα, η απαίτηση του σημείου 4.10 καλύπτεται από λύσεις που παρέχουν:

- Αυτόματη ανάλυση και συσχέτιση περιστατικών με AI
- Προτεινόμενες ενέργειες απόκρισης (AI-generated recommendations)
- Executive summaries για διοίκηση σε μη τεχνική γλώσσα
- AI-assisted root cause analysis
- Predictive analytics για προληπτική ανίχνευση απειλών

Η λειτουργική αυτή κάλυψη θεωρείται επαρκής, ανεξαρτήτως της συγκεκριμένης υλοποίησης (LLM, ML, NLP).

Ερώτημα 60ο:

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΑΣ ΣΥΜΜΟΡΦΩΣΗΣ

Σημείο 19:

Η προσφερόμενη λύση θα πρέπει να είναι του ιδίου κατασκευαστή με την προσφερόμενη λύση των NGFW, της λύσης προστασίας ηλεκτρονικού ταχυδρομείου, της λύσης ολοκληρωμένης ασφάλειας identity and access management για καλύτερη διαλειτουργικότητα.

Η απαίτηση η προσφερόμενη λύση να είναι του ιδίου κατασκευαστή με τις λύσεις NGFW, προστασίας ηλεκτρονικού ταχυδρομείου και identity and access management εισάγει περιορισμό συγκεκριμένου κατασκευαστή και ενδέχεται να αποκλείει λύσεις που πληρούν ισοδύναμα τις απαιτήσεις μέσω διαλειτουργικότητας. Παρακαλείται να διευκρινιστεί εάν η απαίτηση δύναται να απαλειφθεί ή να αναδιατυπωθεί. Προτείνεται η αντικατάστασή της με απαίτηση διασφάλισης διαλειτουργικότητας και ολοκλήρωσης σε επίπεδο προτύπων και διεπαφών (APIs), ανεξαρτήτως κατασκευαστή, ώστε να επιτρέπονται ισοδύναμες λύσεις και να ενισχύεται ο ανταγωνισμός.

Απάντηση:

Η τεχνική προσφορά του αναδόχου πρέπει να είναι συμβατή με τους όρους της διακήρυξης.

Ερώτημα 61ο:

1. Διάρκεια αδειών, συνδρομών, εγγυήσεων και υπηρεσιών υποστήριξης

Στη σελίδα 2 της Διακήρυξης, στα Συνοπτικά Στοιχεία Έργου, αναφέρεται ότι η διάρκεια της σύμβασης είναι τριάντα έξι (36) μήνες.

Περαιτέρω, στη σελίδα 8 της Διακήρυξης, καθώς και στην παράγραφο 6.2.1 στη σελίδα 69, αναφέρεται ότι η συνολική διάρκεια της σύμβασης ορίζεται σε τριάντα έξι (36) μήνες από την ημερομηνία υπογραφής της σύμβασης, πλην όμως στον ανωτέρω χρόνο δεν συμπεριλαμβάνονται οι χρόνοι παραλαβής των παραδοτέων.

Επιπλέον, στο Υπόδειγμα Οικονομικής Προσφοράς, στη σελίδα 163, το Μέρος Γ «Υπηρεσίες Υποστήριξης & Λειτουργίας» αναφέρεται σε διάρκεια τριάντα έξι (36) μηνών, ενώ στην ίδια σελίδα το Μέρος Δ.1 «Λογισμικό και Τεχνολογικές Λύσεις – Άδειες Λογισμικού» αναφέρεται επίσης σε τριάντα έξι (36) μήνες και σε συνολικό κόστος 3ετίας. Αντίστοιχα, στη σελίδα 164, στον Συγκεντρωτικό Πίνακα Οικονομικής Προσφοράς, τα Μέρη Γ και Δ.1 αναφέρονται εκ νέου ως διάρκειας τριάντα έξι (36) μηνών.

Λαμβάνοντας υπόψη τα ανωτέρω, παρακαλούμε να διευκρινιστεί ρητώς εάν οι προσφερόμενες άδειες, συνδρομές, εγγυήσεις, υπηρεσίες τεχνικής υποστήριξης, υπηρεσίες συντήρησης και εν γένει οι υπηρεσίες που συνδέονται με τις προσφερόμενες λύσεις θα πρέπει να καλύπτουν αποκλειστικά διάρκεια τριάντα έξι (36) μηνών ή εάν, λόγω μη συνυπολογισμού των χρόνων παραλαβής στη συμβατική διάρκεια, απαιτείται κάλυψη για

μεγαλύτερη περίοδο, ήτοι έως σαράντα δύο (42) μήνες. Σε περίπτωση που απαιτείται κάλυψη σαράντα δύο (42) μηνών ή οποιασδήποτε περιόδου πέραν των τριάντα έξι (36) μηνών, παρακαλούμε να διευκρινιστεί:

α) εάν η πρόσθετη περίοδος αφορά χρόνο παραλαβής, περίοδο υλοποίησης, περίοδο μετάβασης, περίοδο εγγύησης, περίοδο παραγωγικής λειτουργίας ή άλλη συμβατική υποχρέωση,

β) εάν η οικονομική προσφορά θα πρέπει να υπολογιστεί με βάση διάρκεια 36 ή 42 μηνών, και

γ) εάν όλες οι άδειες λογισμικού, συνδρομές και υπηρεσίες υποστήριξης θα πρέπει να είναι ενεργές καθ' όλη την τυχόν πρόσθετη περίοδο.

Απάντηση:

Οι απαιτούμενες άδειες θα πρέπει να έχουν διάρκεια 36 μηνών και με βάση αυτή την διάρκεια θα πρέπει να υποβληθεί η οικονομική προσφορά του Αναδόχου

Ερώτημα 62ο:

2. Προδιαγραφή 19 του Πίνακα Δ.1.1 – Απαίτηση ίδιου κατασκευαστή και διαλειτουργικότητα λύσεων

Στον Πίνακα Συμμόρφωσης Δ.1.1, που αφορά τη Λύση Κεντρικής Πλατφόρμας Ενορχήστρωσης Ασφαλείας, Αυτοματοποίησης και Απόκρισης (SOAR), και ειδικότερα στην προδιαγραφή 19, αναφέρεται ότι:

«Η προσφερόμενη λύση θα πρέπει να είναι του ιδίου κατασκευαστή με την προσφερόμενη λύση των NGFW, της λύσης προστασίας ηλεκτρονικού ταχυδρομείου, της λύσης ολοκληρωμένης ασφάλειας identity and access management για καλύτερη διαλειτουργικότητα».

Παρακαλούμε να διευκρινιστεί εάν η ανωτέρω απαίτηση αποτελεί υποχρεωτικό και απαράβατο όρο, υπό την έννοια ότι η προσφερόμενη λύση SOAR, η λύση NGFW, η λύση προστασίας ηλεκτρονικού ταχυδρομείου και η λύση identity and access management πρέπει υποχρεωτικά να προέρχονται από τον ίδιο κατασκευαστή.

Απάντηση:

Η τεχνική προσφορά του αναδόχου πρέπει να είναι συμβατή με τους όρους της διακήρυξης.

Ερώτημα 63ο:

3. Χρήση αγγλικών όρων και αγγλικού κειμένου σε τεχνικές προδιαγραφές

Κατά τη μελέτη των τεχνικών προδιαγραφών διαπιστώνεται ότι σε αρκετά σημεία της Διακήρυξης και των Πινάκων Συμμόρφωσης περιλαμβάνονται αγγλικοί όροι, τεχνικές διατυπώσεις ή μικτό ελληνικό και αγγλικό κείμενο, όπως :

Π.χ. Βλέπε παράγραφο 3.1.2.6. Α.6 Perimeter Security (σελίδα 84)

• Next-Generation Firewalls (NGFW) με Deep Packet Inspection και application-aware κανόνες
On-Premises: Η υπηρεσία NGFW deployment στα 150 σημεία προσφέρεται από τα 2 κεντρικά NGFW με unified threat management, deep packet inspection για εισερχόμενη και εξερχόμενη κίνηση, application control για Microsoft και Oracle applications, και centralized policy management για consistent security posture.

Cloud: Native cloud firewall services (Azure Firewall Premium, OCI Network Firewall) με cloudnative threat intelligence, auto-scaling capabilities, και seamless integration με cloud networking services. Απαιτείται consistent policy enforcement μεταξύ on-premises και cloud perimeters.

• Web Application Firewalls (WAF) με OWASP Top 10 προστασία και machine learning
On-Premises: Η υπηρεσία WAF για προστασία των εσωτερικών web applications του Κτηματολογίου, προσφέρεται από τα κεντρικά WAF συστήματα με custom rule sets για Oraclebased applications, real-time attack mitigation, SQL injection και XSS protection, και bot management capabilities.
Cloud: Cloud-native WAF services (Azure Application Gateway WAF, OCI WAF) για cloud- hosted applications με machine learning-based threat detection, API protection, DDoS mitigation, και global threat intelligence updates.

• Δικτυακά IDS/IPS με signature-based και anomaly-based detection
On-Premises: Network-based IDS/IPS με real-time monitoring εισερχόμενης κίνησης στο perimeter, signature-based detection για γνωστές απειλές, behavioral analysis για zero-day attacks, και automated blocking capabilities με fine-tuned false positive management.
Cloud: Cloud-native IDS/IPS με machine learning-enhanced detection, container και serverless workload protection, API traffic analysis, και cross-cloud threat correlation με automated response capabilities.

• Διαχωρισμός ζωνών (Network Segmentation & DMZs) με micro-segmentation
On-Premises: Δημιουργία DMZ zones για public-facing services, strict segmentation μεταξύ internal και external networks, secure zones για Oracle database access, και guest network isolation. Υλοποίηση micro-segmentation για granular control της κίνησης μεταξύ zones.
Cloud: Cloud-native zone isolation με VNets/VCNs, security groups, και network policies. Multitier architecture με separate zones για web, application, και database layers. Cross-cloud zone policies για hybrid applications που εκτείνονται σε multiple cloud environments.

• DDoS Protection Systems με always-on προστασία και automatic traffic scrubbing
On-Premises: On-premises DDoS protection με traffic analysis, automatic mitigation, και integration με upstream ISP services. Rate limiting, traffic shaping, και emergency response procedures για volumetric attacks που στοχεύουν τις εσωτερικές υπηρεσίες.
Cloud: Cloud-native DDoS protection (Azure DDoS Protection, OCI DDoS Protection) με global scrubbing centers, machine learning-based attack detection, automatic scaling κατά τη διάρκεια attacks, και real-time attack analytics και reporting.

• VPN για ασφαλή απομακρυσμένη πρόσβαση με MFA και endpoint compliance
On-Premises: Η υπηρεσία SSL VPN και IPsec VPN για remote access στις εσωτερικές υπηρεσίες, site-to-site VPN για secure connectivity μεταξύ των 150 τοποθεσιών θα προσφέρεται μέσω των κεντρικών NGFW. Παράλληλα θα παραμετροποιηθεί integration με Microsoft AD για authentication, και endpoint compliance checking πριν το access των χρηστών στο VPN.
Cloud: Cloud VPN services για secure access σε cloud resources, point-to-site VPN για remote users, ExpressRoute/FastConnect για dedicated connectivity μέσω ΓΓΠΣ, και cloud-based VPN management με centralized policies και monitoring.

• Anti-spam/Anti-malware gateways για email & web traffic με sandboxing και URL filtering
On-Premises: Email security gateways για inbound/outbound email filtering, web security gateways για HTTP/HTTPS traffic inspection, advanced sandboxing για suspicious attachments και URLs, και integration με threat intelligence feeds για real-time protection.
Cloud: Cloud-based email security (Microsoft Defender for Office 365, third-party solutions) και web security services με global threat intelligence, machine learning-based detection, και seamless integration με cloud productivity suites και applications.

Π.χ. Βλέπε παράγραφο 3.1.4.1. Γ.1 Λειτουργικές Υπηρεσίες σελ.94-95 της διακήρυξης:

Security Operations Center (SOC)

• 24/7/365 Παρακολούθηση Ασφάλειας Εσωτερικής Υποδομής και Cloud Εφαρμογών
Οι υπηρεσίες SOC πρέπει να περιλαμβάνουν συνεχή παρακολούθηση των on-premises συστημάτων (Oracle DB 19c, Microsoft AD, εσωτερικό δίκτυο) και των cloud environments (Oracle OCI, Microsoft Azure μέσω ΓΓΠΣ). Απαιτείται 24/7/365 coverage από έμπειρο security analysts, tier 1/2/3 escalation procedures, real-time threat detection και response για hybrid infrastructure.

• Security Event Management και Incident Response
Το SOC πρέπει να παρέχει comprehensive incident classification και response, forensic investigation capabilities, threat hunting activities για advanced persistent threats, και integration με όλα τα security tools (SIEM, EDR, firewalls). Απαιτείται διαχείριση security incidents που επηρεάζουν τόσο εσωτερικά όσο και cloud συστήματα.
• Threat Intelligence και Advanced Analytics
Οι υπηρεσίες SOC πρέπει να περιλαμβάνουν threat intelligence integration, behavioral analytics, και proactive threat hunting για identification advanced attacks που στοχεύουν hybrid environments. Απαιτείται correlation των events μεταξύ on-premises και cloud platforms.
Network Operations Center (NOC)
• Παρακολούθηση Εσωτερικής Δικτυακής Υποδομής
Οι υπηρεσίες NOC εστιάζουν αποκλειστικά στη δικτυακή υποδομή των 150 γεωγραφικών τοποθεσιών, network performance monitoring, connectivity issues, και hardware/software health του εσωτερικού δικτύου. Δεν καλύπτει cloud networking, το οποίο διαχειρίζεται από τα native cloud monitoring tools.
• Network Change Management και Configuration
Οι υπηρεσίες NOC πρέπει να περιλαμβάνουν change management για δικτυακές αλλαγές, configuration management των switches/routers/firewalls, network capacity planning, και proactive maintenance του εσωτερικού δικτύου. Συντονισμός με IT teams για planned maintenance windows.
• Network Performance Optimization και Reporting
Το NOC πρέπει να παρέχει continuous network monitoring, performance optimization για WAN/LAN connectivity, bandwidth management, και detailed reporting για network availability και performance metrics. Εστίαση στην εσωτερική connectivity μεταξύ των κεντρικών και περιφερειακών γραφείων.
Κοινές Υπηρεσίες SOC & NOC
• Continuous Improvement και Optimization
Και τα δύο centers πρέπει να παρέχουν continuous improvement processes, lessons learned integration, και regular optimization των procedures και tools για αύξηση της efficiency και effectiveness.
• Reporting και Metrics
Απαιτείται comprehensive reporting για SOC (security metrics, incident reports, threat intelligence) και NOC (network performance, availability, capacity utilization) με executive dashboards και detailed technical reports.
• Automated Response & Orchestration (SOAR)
Υλοποίηση automation workflows για routine tasks, automated incident response procedures, και orchestration μεταξύ SOC και NOC για incidents που επηρεάζουν τόσο security όσο και network operations.

Παρακαλούμε να διευκρινιστεί εάν οι αγγλικοί όροι και οι αγγλικές διατυπώσεις έχουν χρησιμοποιηθεί αποκλειστικά ως διεθνώς καθιερωμένη τεχνική ορολογία ή εάν παραπέμπουν σε συγκεκριμένες τεχνολογικές λειτουργίες, προϊόντα, εμπορικές ονομασίες, υλοποιήσεις ή τεχνικές αρχιτεκτονικές συγκεκριμένων κατασκευαστών.

Περαιτέρω, παρακαλούμε να διευκρινιστεί ότι, σε περίπτωση ασάφειας ή διαφορετικής ερμηνείας μεταξύ ελληνικής και αγγλικής διατύπωσης, η συμμόρφωση θα αξιολογηθεί με βάση την ουσιαστική τεχνική λειτουργικότητα που ζητείται και όχι με βάση συγκεκριμένη ονομασία, εμπορική διατύπωση ή ακριβή λεκτική αντιστοίχιση αγγλικού όρου.

Τέλος, παρακαλούμε να επιβεβαιωθεί ότι γίνονται αποδεκτές ισοδύναμες τεχνικές προσεγγίσεις, εφόσον ο προσφέρων τεκμηριώνει ότι καλύπτουν πλήρως το λειτουργικό αποτέλεσμα που περιγράφεται στις σχετικές προδιαγραφές ή διαφορετικά να διευκρινίσετε με αντίστοιχο ελληνικό κείμενο.

Απάντηση:

Βλέπε απάντηση ερωτήματος 20.

Ερώτημα 64ο:

4. Τυχόν τροποποίηση όρων της Διακήρυξης και απαιτούμενες διατυπώσεις Δημοσιότητας

Σε περίπτωση που, κατόπιν των ανωτέρω διευκρινίσεων, προκύψει ανάγκη τροποποίησης, συμπλήρωσης ή αναδιατύπωσης όρων της Διακήρυξης ή των Πινάκων Συμμόρφωσης, παρακαλούμε να διευκρινιστεί εάν οι εν λόγω τροποποιήσεις θα θεωρηθούν ουσιώδεις, ιδίως εφόσον επηρεάζουν ελάχιστες απαιτήσεις όπως τη διάρκεια των ζητούμενων αδειών/συνδρομών, τη διαμόρφωση της οικονομικής προσφοράς, τις τεχνικές απαιτήσεις συμμετοχής ή τη δυνατότητα προσφοράς ισοδύναμων λύσεων.

Στην περίπτωση ουσιώδους τροποποίησης των όρων της Διακήρυξης, παρακαλούμε να επιβεβαιωθεί ότι θα τηρηθούν οι προβλεπόμενες διατυπώσεις δημοσιότητας, ήτοι η δημοσίευση στο ΚΗΜΔΗΣ και, εφόσον πρόκειται για διαδικασία που εμπίπτει στο αντίστοιχο πεδίο εφαρμογής, στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, καθώς και ότι θα χορηγηθεί επαρκής παράταση της προθεσμίας υποβολής προσφορών με την νέα διακήρυξη.

Η ανωτέρω διευκρίνιση ζητείται λαμβάνοντας υπόψη τη σχετική νομολογία, σύμφωνα με την οποία, όταν μεταβάλλονται ουσιωδώς όροι διεξαγωγής διαγωνιστικής διαδικασίας, δεν αρκεί απλή ανάρτηση ή ενημέρωση μέσω της πλατφόρμας, αλλά απαιτείται η τήρηση των προβλεπόμενων διατυπώσεων δημοσιότητας. Ενδεικτικώς αναφέρονται η απόφαση ΣτΕ 1792/2024, σκ. 7, καθώς και η Πράξη ΕλΣυν Ζ΄ Κλιμ. 25/2025, η οποία αφορά ουσιώδη τροποποίηση όρων διαγωνισμού και την ανάγκη τήρησης των απαιτούμενων δημοσιεύσεων.

Απάντηση:

Θα τηρηθούν οι όροι διεξαγωγής της διαγωνιστικής διαδικασίας.

Η Γενική Διευθύντρια

OLYMPIA MARKELLOU
16.07.2026 15:30

Ολυμπία Μαρκέλλου