



Αθήνα, 02/03/2026

Αρ. πρωτ. 3827/ΑΣ

Διευκρινίσεις στα σχόλια που υποβλήθηκαν κατά τη διενέργεια Δημόσιας Διαβούλευσης Τεύχους Διακήρυξης Ηλεκτρονικού Ανοικτού Διαγωνισμού Άνω των Ορίων για Σύναψη Συμφωνίας Πλαίσιο για το Υποέργο 1 «Ενίσχυση της κυβερνοασφάλειας των ΟΤΑ Α' βαθμού» του Έργου «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ» της Πράξης «Προμήθεια εξοπλισμού και υπηρεσιών Κυβερνοασφάλειας για τους ΟΤΑ» με κωδικό ΟΠΣ (MIS) 5225494.

ΣΧΟΛΙΟ 1	ΑΠΑΝΤΗΣΗ	ΑΛΛΑΓΗ ΝΑΙ/ΟΧΙ
<p>2.2.6.1 Τεχνική Ικανότητα</p> <p>Παρακαλούμε να αφαιρεθούν τα εξής από την παρακάτω απαίτηση:</p> <p>"Έως έξι (6) έργα που έχουν συνολικό προϋπολογισμό τουλάχιστον ενός εκατομμυρίου ευρώ (1.000.000 €) και περιλαμβάνουν αθροιστικά τα κάτωθι αντικείμενα:</p> <ul style="list-style-type: none">ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) Συστήματος Διαχείρισης Ασφάλειας Πληροφοριώνο Σχεδιασμό ή/και συντήρηση (υποστήριξη) πλάνου ανάκαμψης από καταστροφή ή/και Συστήματος διαχείρισης επιχειρησιακής συνέχειαςο Διενέργεια ελέγχων παρεϊσδυσης (penetration test)ο Εκπόνηση μελέτης αξιολόγησης κινδύνωνο Εκπόνηση προτάσεων για την ασφάλεια συστημάτωνο Παροχή υπηρεσιών εκπαίδευσης ή/και ευαισθητοποίησης για την κυβερνοασφάλεια με χρήση πλατφόρμας εκπαίδευσηςο Πιστοποιημένες εκπαιδεύσεις στην ασφάλεια πληροφοριών ή/και την επιχειρησιακή συνέχειαο Προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και εγκατάσταση του εν λόγω εξοπλισμού σε τουλάχιστον τριάντα (30) σημεία με γεωγραφική διασπορά σε τουλάχιστον έξι (6) περιφέρειες.ο Υλοποίηση τουλάχιστον τριών (3) από τις παρακάτω λύσεις κυβερνοασφάλειας:<ul style="list-style-type: none">▪ Υποσύστημα SIEM με αξιοποίηση AI αλγόριθμων.▪ Υποσύστημα δημιουργίας για honeypots.▪ Υποσύστημα στατική ανάλυση κώδικα.▪ Προστασία Ηλεκτρονικού Ταχυδρομείου / Secure Mail Gateway	<p>Η απαίτηση για μέγιστο αριθμό έργων έχει ουσιαστικό σκοπό να διασφαλίσει ότι τα έργα που θα επικαλεστούν οι υποψήφιοι θα είναι ανάλογου μεγέθους και πολυπλοκότητας με το παρόν έργο. Για τη διευκόλυνση των υποψηφίων η απαίτηση επανακαθορίζεται σε έως οχτώ (8) έργα, με συνολικό προϋπολογισμό τουλάχιστον ενός εκατομμυρίου ευρώ (1.000.000) .</p> <p>Ειδικά για την απαίτηση για πιστοποιημένες εκπαιδεύσεις, η απαίτηση παραμένει εφόσον σχετίζεται με το φυσικό αντικείμενο, καθώς οι πιστοποιημένες εκπαιδεύσεις εντάσσονται στο φυσικό αντικείμενο του έργου, όπως αναφέρεται στο σημείο 2 Του κεφαλαίου 2.3 του Παραρτήματος Ι της διακήρυξης. Εξάλλου, η πιστοποίηση στελεχών αποτελεί σημαντική παράμετρο για την ενδυνάμωση της κυβερνοασφάλειας στους ΟΤΑ.</p>	ΝΑΙ

<p>▪ Προστασία Τελικού Σημείου"</p> <p>Να αφαιρεθεί ο περιορισμός των 6 έργων καθώς δεν εξυπηρετεί ουσιαστικό σκοπό και περιορίζει αδικαιολόγητα τη δυνατότητα τεκμηρίωσης εμπειρίας από υποψηφίους που έχουν υλοποιήσει περισσότερα έργα μικρότερης αξίας, τα οποία αθροιστικά υπερκαλύπτουν τον απαιτούμενο συνολικό προϋπολογισμό και τα ζητούμενα αντικείμενα.</p> <p>Επιπλέον, παρακαλούμε να αφαιρεθεί και η απαίτηση στα έργα για "Πιστοποιημένες εκπαιδεύσεις στην ασφάλεια πληροφοριών ή/και την επιχειρησιακή συνέχεια" καθώς η τεχνική και επαγγελματική επάρκεια διασφαλίζεται από τα υπόλοιπα αντικείμενα και τις λοιπές απαιτήσεις.</p>		
<p>2.2.6.2 Επαγγελματική Ικανότητα – Ομάδα Έργου</p> <p>- Παρακαλούμε να αφαιρεθεί η απαίτηση στον ρόλο του Υπεύθυνου Έργου:</p> <p>"Να είναι κάτοχος πιστοποίησης στη διαχείριση υπηρεσιών πληροφορικής (ITIL ή αντίστοιχη ή ισοδύναμη)"</p> <p>Η πιστοποίηση στη διαχείριση έργων (PMI, PRINCE2, PM2 ή ισοδύναμη) είναι επαρκής για τη διασφάλιση της επαγγελματικής ικανότητας του Υπεύθυνου Έργου. Η πιστοποίηση ITIL αφορά κυρίως τη διαχείριση υπηρεσιών πληροφορικής (IT Service Management) και όχι τη διαχείριση έργων, που είναι το βασικό αντικείμενο του ρόλου του Υπεύθυνου Έργου.</p>	<p>Η απαίτηση αφαιρείται</p>	<p>ΝΑΙ</p>
<p>2.2.7 Πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης</p> <p>- Παρακαλούμε να αφαιρεθεί η απαίτηση για:</p> <p>"ISO 29993:2017 ή άλλο ισοδύναμο εν ισχύ για την παροχή υπηρεσιών εκπαίδευσης."</p> <p>Το ISO 29993:2017 αφορά αποκλειστικά ανεξάρτητες υπηρεσίες εκπαίδευσης εκτός του τυπικού εκπαιδευτικού συστήματος και δεν αποτελεί ευρέως διαδεδομένο ή υποχρεωτικό πρότυπο για παρόχους εκπαιδευτικών υπηρεσιών στον τομέα της πληροφορικής ή της κυβερνοασφάλειας, δεν προσφέρει ουσιαστική προστιθέμενη αξία στο αντικείμενο του έργου, ενώ ενδέχεται να αποκλείσει αξιόλογους υποψηφίους με μεγάλη εμπειρία και διεθνείς πιστοποιήσεις.</p>	<p>Η διενέργεια εκπαιδεύσεων εκτός του τυπικού εκπαιδευτικού συστήματος αποτελεί μέρος του φυσικού αντικειμένου του έργου και κρίσιμη παράμετρο για την ενδυνάμωση των ΟΤΑ και κατά συνέπεια η απαίτηση παραμένει.</p>	<p>ΟΧΙ</p>
<p>- Παρακαλούμε να γίνουν οι εξής τροποποιήσεις στην απαίτηση:</p> <p>"Επιπλέον, ο Υπεύθυνος ομάδας υπηρεσιών ασφάλειας και ο Αναπληρωτής Υπεύθυνος ομάδας υπηρεσιών ασφάλειας αθροιστικά πρέπει να κατέχουν τις ακόλουθες ή ισοδύναμες πιστοποιήσεις:</p> <ul style="list-style-type: none"> ▪ ISO 27001 Lead Auditor ▪ Certified Information Security Manager (CISM) ▪ Business Continuity Certified Lead Auditor ▪ Data Protection Officer (DPO) ▪ ITIL® Foundation in IT Service Management. ▪ Certified Information Privacy Professional /Europe (CIPP/E)" <p>Παρακαλούμε να υπάρχει η δυνατότητα οι ζητούμενες πιστοποιήσεις να μπορούν να καλύπτονται αθροιστικά από τα δύο στελέχη</p>	<p>Διευκρινίζεται ότι η απαίτηση για τις σχετικές πιστοποιήσεις ζητείται να καλύπτεται αθροιστικά από τα δύο (2) στελέχη, παρέχοντας ευελιξία στους υποψηφίους.</p> <p>Η πιστοποίηση CIPP/E αντιστοιχεί σε θεωρητικό υπόβαθρο ενώ η αντίστοιχη για DPO σε πρακτικά εφόδια για την εκπλήρωση του ρόλου, έτσι ώστε οι δύο πιστοποιήσεις να αλληλοσυμπληρώνονται.</p>	<p>ΟΧΙ</p>

<p>(Υπεύθυνο και Αναπληρωτή), καθώς το ότι κάθε στέλεχος να διαθέτει όλες τις πιστοποιήσεις, είναι εξαιρετικά περιοριστικό και δεν ανταποκρίνεται στην πραγματικότητα της αγοράς.</p> <p>Επιπλέον, παρακαλούμε να αφαιρεθεί πλήρως η απαίτηση για "Certified Information Privacy Professional /Europe (CIPP/E)" καθώς δεν αποτελεί ευρέως διαδεδομένο ή ουσιώδες κριτήριο για την υλοποίηση έργων κυβερνοασφάλειας στο δημόσιο τομέα, ενώ η απαίτηση για DPO (Data Protection Officer) καλύπτει επαρκώς το αντικείμενο της προστασίας προσωπικών δεδομένων.</p>		
<p>- Παρακαλούμε να αφαιρεθεί τελείως η παρακάτω απαίτηση: "Δύο (2) στελέχη σε ρόλο συμβούλων ασφάλειας το καθένα εκ των οποίων να διαθέτει: ο Πανεπιστημιακό τίτλο σπουδών ή/και Μεταπτυχιακό τίτλο σπουδών ο Τουλάχιστον 3ετή εμπειρία σε έργα συμβουλευτικών υπηρεσιών ή/και ανάπτυξης, εγκατάστασης και εφαρμογής Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ή/και σε έργα ανάλυσης, αξιολόγησης κινδύνων (risk analysis & assessment). Καθένα από τα στελέχη έργου σε ρόλο συμβούλων ασφάλειας θα πρέπει να κατέχει τις εξής ή ισοδύναμες πιστοποιήσεις: ο ISO 27001:2013 ο CompTIA security+" Η συγκεκριμένη απαίτηση είναι υπερβολικά εξειδικευμένη και περιορίζει αδικαιολόγητα τον ανταγωνισμό, καθώς συνδυάζει ακαδημαϊκά προσόντα, εμπειρία και συγκεκριμένες πιστοποιήσεις για δύο στελέχη, ενώ οι σχετικές αρμοδιότητες καλύπτονται ήδη από τα βασικά στελέχη της ομάδας έργου (Υπεύθυνος και Αναπληρωτής Υπεύθυνος ομάδας υπηρεσιών ασφάλειας). Η ύπαρξη εξειδικευμένων συμβούλων ασφάλειας με ταυτόχρονη κατοχή ISO 27001:2013 και CompTIA Security+ δεν αποτελεί συνήθη πρακτική σε αντίστοιχα έργα του δημοσίου και δεν προσφέρει ουσιαστική προστιθέμενη αξία, δεδομένου ότι η συνολική τεχνική επάρκεια της ομάδας διασφαλίζεται από τις υπόλοιπες απαιτήσεις. Η διατήρηση της απαίτησης αυτής ενδέχεται να αποκλείσει αξιόλογους υποψηφίους και να μειώσει τον υγιή ανταγωνισμό.</p>	<p>Η εν λόγω πιστοποίηση είναι τεχνικού χαρακτήρα και εξασφαλίζει επαρκή γνώση των συμβούλων, ώστε να επιτελέσουν τον ρόλο τους στην υλοποίηση του έργου. Για τη διευκόλυνση των υποψηφίων η απαίτηση τροποποιείται και οι πιστοποιήσεις ζητούνται αθροιστικά από τα δύο (2) στελέχη, ενώ προστέθηκε και η πιστοποίηση ISC² Certified in Cybersecurity (CC) ως αποδεκτή ισοδύναμη πιστοποίηση.</p>	<p>ΝΑΙ</p>
<p>2.2.6.1 Τεχνική Ικανότητα - 2.3 Απαιτήσεις και Τεχνικές Προδιαγραφές - 2.ΠΑΡΑΡΤΗΜΑ ΙΙ – ΠΙΝΑΚΕΣ ΣΥΜΜΟΡΦΩΣΗΣ4 Απαιτήσεις Ομάδων Έργου Δεν υπάρχει αναφορά στην υποδομή SOC που πρέπει να διαθέτει ο Ανάδοχος, ώστε να προσφέρει τις υπηρεσίες SOC. Δεδομένης της βαρύτητας της υπηρεσίας SOC κρίνεται απαραίτητο να προστεθούν συγκεκριμένα κριτήρια για την υποδομή SOC του Αναδόχου όπως: Να διαθέτει δύο (2) τουλάχιστον SOCs (είτε πλήρους ιδιοκτησίας του, είτε μέσω μόνιμης εταιρικής σχέσης ή συνεργασίας η οποία πρέπει να αποδεικνύεται εγγράφως) και να εξασφαλίζεται παρακολούθηση 24x7x365, με: • Τουλάχιστον 2 ομάδες SOC σε παγκόσμιο επίπεδο • Το κύριο SOC να βρίσκεται εντός της Ευρωπαϊκής Ένωσης. Το κύριο SOC θα πρέπει να είναι πλήρους και αποκλειστικής ιδιοκτησίας του υποψήφιου Αναδόχου.</p>	<p>Προστέθηκε πίνακας συμμόρφωσης "8. Υπηρεσία Security Operations Center", όπου αναφέρονται με μεγαλύτερη λεπτομέρεια οι απαιτήσεις σχετικά με την υπηρεσία SOC</p>	<p>ΝΑΙ</p>

<p>Δεδομένης της έκτασης και κρισιμότητας του έργου κρίνεται απαραίτητο να τεθούν αυστηρά κριτήρια για τις SOC υπηρεσίες, ώστε να διασφαλιστεί απρόσκοπτη και υψηλού επιπέδου υπηρεσία.</p>		
<p>Στη παράγραφο 2.3 δίνεται μόνο ο αριθμός του πληθυσμού ανά μέγεθος Δήμου και συγκεκριμένα στη παράγραφο 6. Υπηρεσίες SOC (Security Operation Center) σελ. 113 περιγράφονται πολύ γενικά χαρακτηριστικά μιας SOC υπηρεσίας. Κρίνεται απαραίτητο να δοθεί μια τάξη μεγέθους των παρακάτω στοιχείων ανά μέγεθος Δήμου</p> <ul style="list-style-type: none"> • Αριθμός υπαλλήλων του Δήμου • Αριθμός τερματικών του Δήμου • Αριθμός servers του Δήμου • Εκτιμώμενος αριθμός EPS ή εκτιμώμενος αριθμός ανάλυσης (ingestion) GB/day <p>Κρίνεται απαραίτητο να οριστούν συγκεκριμένα κριτήρια για την ομάδα SOC του Αναδόχου Δεν περιλαμβάνει Πίνακα Συμμόρφωσης για τη SOC υπηρεσία. Δεδομένης της κρισιμότητας του έργου και της απαιτητικής υπηρεσίας SOC που θα κληθεί ο Ανάδοχος να προσφέρει κρίνεται απαραίτητο να συμπεριληφθεί αναλυτικός Πίνακας Συμμόρφωσης καλύπτοντας τις παρακάτω ενότητες και λαμβάνοντας υπόψιν παιδιά όπως sizing, technological stack, SLA, SOC ομάδα, κλπ.</p> <ul style="list-style-type: none"> • Υπηρεσίες Αρχικής Υλοποίησης • Γενικά Απαιτήσεις Υπηρεσίας SOC • Δυνατότητες SOAR και Αναφορών • Υπηρεσία SOC για τερματικά και servers • Υπηρεσία SOC για on-prem, cloud και υβριδική υποδομή • Υπηρεσίες Ψηφιακής Διερεύνησης και Αντιμετώπισης Περιστατικών 	<p>Προστέθηκε πίνακας συμμόρφωσης "8. Υπηρεσία Security Operations Center", όπου αναφέρονται με μεγαλύτερη λεπτομέρεια οι απαιτήσεις σχετικά με την υπηρεσία SOC</p>	<p>ΝΑΙ</p>
<p>2.2.6.1 Τεχνική Ικανότητα Δεν υπάρχει αναφορά σε έργα SOC. Δεδομένης της βαρύτητας της υπηρεσίας SOC κρίνεται απαραίτητο να προστεθεί απαίτηση για ολοκλήρωση SOC έργων. Όπως για παράδειγμα: Να έχει ολοκληρώσει επιτυχώς Χ έργα υπηρεσιών MDR (Managed Detection and Response) / SOC (Security Operations Center), το συμβατικό τίμημα των οποίων αθροιστικά να ισούται με το xx% του προϋπολογισμού του παρόντος έργου (χωρίς ΦΠΑ).</p>	<p>Προστέθηκε πίνακας συμμόρφωσης "8. Υπηρεσία Security Operations Center", όπου αναφέρονται με μεγαλύτερη λεπτομέρεια οι απαιτήσεις σχετικά με την υπηρεσία SOC. Στον πίνακα συμμόρφωσης ενσωματώθηκε γραμμή με την οποία ζητείται σχετική εμπειρία από τον <i>πάροχο</i> της υπηρεσίας.</p>	<p>ΝΑΙ</p>
<p>Τα Τείχη Προστασίας Νέας Γενιάς (Next Gen Firewall) όλων των οργανισμών τοπικής αυτοδιοίκησης και ανεξάρτητα από την κατηγορία τους (Μεγάλος, Μεσαίος, Μικρός Δήμος) και στο πλαίσιο του έργου πρέπει να έχουν ποιοτικά χαρακτηριστικά για λόγους ενοποιημένης διαχείρισης και ορατότητας, συμβατότητας, ομοιόμορφης υποστήριξης και ενημέρωσης καθώς και την μείωση κόστους με οικονομία κλίμακας και μείωσης της πολυπλοκότητας.</p> <p>Σε αυτό το πλαίσιο και λαμβάνοντας υπόψιν τις επιμέρους προδιαγραφές, την διαμόρφωση του σύγχρονου περιβάλλοντος κυβερνοασφάλειας και απειλών καθώς και τις κατηγορίες Μεγάλος, Μεσαίος, Μικρός Δήμος προτείνουμε ότι ο Πίνακας Προδιαγραφών «Τείχος Προστασίας Επόμενης Γενιάς για Μεγάλους Δήμους» πρέπει</p>	<p>Οι αλλαγές ενσωματώθηκαν στους αντίστοιχους πίνακες συμμόρφωσης</p>	<p>ΝΑΙ</p>

<p>να αντιστοιχηθεί στον Πίνακα Προδιαγραφών «Τείχος Προστασίας Επόμενης Γενιάς για Μικρούς και Μεσαίους Δήμους». Αντίστοιχα στον Πίνακα Προδιαγραφών «Τείχος Προστασίας Επόμενης Γενιάς για Μεγάλους Δήμους» πρέπει να γίνουν αλλαγές ώστε τα προτεινόμενα Τείχη Προστασίας να αντικατοπτρίζουν τόσο το μέγεθος του Μεγάλου Δήμου σε όγκο δεδομένων αλλά και νέων απειλών ως εξής:</p> <p>«Τείχος Προστασίας Επόμενης Γενιάς για Μεγάλους Δήμους»</p> <ul style="list-style-type: none"> - Προσθήκη προδιαγραφή για 2x SFP+ 1/10Gbps Ethernet ανά Τείχος Προστασίας - Προδιαγραφή 10: Ελάχιστο throughput για λειτουργία firewall (FW) με αναγνώριση εφαρμογών (AVC). Να αναφέρεται σε HTTP sessions με μέσο όρο μεγέθους των πακέτων να είναι 1024 bytes \geq 9 Gbps - Προδιαγραφή 11: Ελάχιστο throughput για ταυτόχρονη λειτουργία firewall (FW) με αναγνώρισης εφαρμογών (AVC) και IPS. Να αναφέρεται σε HTTP sessions με μέσο όρο μεγέθους των πακέτων να είναι 1024 bytes \geq 9 Gbps - Προδιαγραφή 12: Ρυθμός δημιουργίας νέων συνδέσεων (connections per second) ανά συσκευή \geq 50.000 - Προδιαγραφή 13: Αριθμός ταυτόχρονων συνδέσεων (concurrent sessions) ανά συσκευή \geq 300.000 - Προδιαγραφή 14: IPSec VPN throughput (για πακέτα 1024bytes TCP) \geq 10 Gbps 		
<p>Πίνακας Συμμόρφωσης "6 Ασφαλής Υπηρεσία Πρόσβασης Άκρου / Secure Access Service Edge (SASE)"</p> <p>Με βάση το SASE framework, η SASE αρχιτεκτονική αποτελείται από ZTNA, SWG/Cloud Proxy, CASB, Cloud Firewall και Secure Edge επιβολή πολιτικών μέσω agent ή identity-based traffic steering (ZTNA) κάτι το οποίο δεν διακρίνεται ξεκάθαρα μέσα στις προδιαγραφές ως απαιτούμενο.</p> <p>Παρακάτω παραθέτουμε κάποιες βασικές απαιτήσεις για λύσεις SASE που προτείνουμε να ενσωματωθούν στις απαιτήσεις ώστε η υπηρεσία να εναρμονίζεται με το SASE Framework:</p> <ol style="list-style-type: none"> 1. Η λύση θα υποστηρίζει επιλογές σύνδεσης μέσω tunnel και proxy 2. Η λύση θα παρέχει δυνατότητες NGFW Firewalling/IPS Filter/App Filter/L7 Inspection & App Control 3. Η λύση θα υποστηρίζει Endpoint Protection (EPP, VPN & ZTNA) στον ίδιο Agent με κοινή διαχείριση. 4. Η λύση θα πρέπει να υποστηρίζει την πρόληψη περιεχομένου (DLP) και το φιλτράρισμα αρχείων για να αποτρέψει την έξοδο ή την είσοδο ευαίσθητων δεδομένων ή αρχείων στο δίκτυο. 5. Η λύση θα πρέπει να υποστηρίζει επιθεώρηση Inline και API-CASB 6. Η λύση πρέπει να είναι σε θέση να εκτελεί έναν έλεγχο κατάστασης (posture) και επίσης να παρακολουθεί συνεχώς τη κατάσταση ασφαλείας του τελικού σημείου ενώ είναι συνδεδεμένο με πόρους τόσο για ασφαλή πρόσβαση στο διαδίκτυο όσο και για 	<p>Οι προδιαγραφές κρίνονται επαρκείς και το σχόλιο δεν γίνεται αποδεκτό.</p>	<p>ΟΧΙ</p>

<p>ασφαλή ιδιωτική πρόσβαση (ztna) χρησιμοποιώντας τους ίδιους ελέγχους κατάστασης. Επιπροσθέτως, οι προδιαγραφές με A/A 8, 51, 52 και 53 δεν αποτελούν χαρακτηριστικά SASE πλατφόρμας, αλλά χαρακτηριστικά cloud DNS υπηρεσιών, που συνήθως λειτουργούν μπροστά από οποιοδήποτε SASE, και ως εκ τούτου προτείνεται να αφαιρεθούν.</p>		
<p>Παράγραφος 2.2.6.2 Οι πιστοποιήσεις Crest είναι περισσότερο προσανατολισμένες στο DORA και τον χώρο των χρηματοοικονομικών, ενώ λείπουν από την λίστα σημαντικές πιστοποιήσεις από την Hack The Box όπως οι Certified Penetration Testing Specialist (CPTS), Certified Web Exploitation Specialist (CWES), Certified Defensive Security Analyst (CDSA). Προτείνουμε την αντικατάσταση ώστε οι πιστοποιήσεις να είναι πιο κοντά στον χώρο των OTA και το αντικείμενο του έργου (CPTS, CWES, CDSA). Επίσης προτείνουμε την διαγραφή των πιστοποιήσεων από την NCSC καθώς είναι Ο Εθνικός φορέας Κυβερνοασφάλειας της Αγγλίας με ρόλο την πιστοποίηση κυρίως για την Αγγλική αγορά.</p>	<p>Ο CREST είναι διεθνής οργανισμός πιστοποίησης και το αντικείμενο των πιστοποιήσεων του δεν είναι προσανατολισμένο στον χρηματοοικονομικό τομέα και απευθύνονται σε οποιοδήποτε επιχειρησιακό περιβάλλον. Οι ζητούμενες πιστοποιήσεις της NCSC ζητούνται για την έμφαση στην ηγεσία ομάδας. Η απαίτηση προσαρμόστηκε έτσι ώστε να ζητείται αθροιστικά μία από τις πιστοποιήσεις και προσφέρεται μία επιπλέον εναλλακτική.</p>	<p>ΝΑΙ</p>
<p>Παράγραφος 2.2.6.2 Οι προδιαγραφές επιλεξιμότητας των βασικών στελεχών του έργου βασίζονται σε ένα σύμπλεγμα πτυχίων, πιστοποιήσεων και προϋπηρεσίας, το σύνολο των οποίων πρέπει να εφαρμόζεται από ένα προτεινόμενο στέλεχος ταυτόχρονα. Έτσι, αδυνατούν να προταθούν στελέχη τα οποία δύναται να διαθέτουν τις πιστοποιήσεις, και την ακαδημαϊκή ή επαγγελματική εμπειρία, αλλά όχι τους πολύ συγκεκριμένους συνδυασμούς αυτών, όπως προβάλλονται στη διακήρυξη. Προτείνουμε τον επαναπροσανατολισμό των απαιτήσεων στις πιστοποιήσεις (προσδιορισμένες ή και ισοδύναμες) των στελεχών, επιτρέποντας μεγαλύτερη ελαστικότητα στα λοιπά προσόντα. Αυτό θα επιτρέψει να μην αποκλειστούν ομάδες έμπειρες με υψηλό επίπεδο τεχνογνωσίας, καταξιωμένες στην αγορά, που τυγχάνει να μην διαθέτουν τους εξαιρετικά ακριβείς συνδυασμούς πτυχίων και πιστοποιήσεων που προδιαγράφονται στο τεύχος ανά στέλεχος.</p>	<p>Είναι σύνηθες για τα στελέχη της ομάδας έργου σε έργα με εξειδικευμένο αντικείμενο να ζητείται συνδυασμός ακαδημαϊκών προσόντων, γενικής εμπειρίας, ειδικής εμπειρίας και πιστοποιήσεων. Ένας τέτοιος συνδυασμός ζητείται σε δεκατρία συνολικά στελέχη, αριθμό ανάλογο με το μέγεθος και την πολυπλοκότητα του έργου, παρέχοντας σε αρκετά σημεία ευελιξία τόσο ως προς τον συνδυασμό πιστοποιήσεων, όσο και ως προς ισοδύναμες πιστοποιήσεις. Οι εν λόγω ζητούμενες πιστοποιήσεις καλύπτουν το πλήρες φάσμα προσόντων για την υλοποίηση των ελέγχων ασφάλειας και ζητούνται αθροιστικά για τα στελέχη, παρέχοντας τη δυνατότητα για ισοδύναμες πιστοποιήσεις. Οι ζητούμενες πιστοποιήσεις έχουν ευρύ πεδίο εφαρμογής και όχι αποκλειστικά την εφαρμογή του κανονισμού DORA ή μόνο για την αγγλική αγορά. Για τη διευκόλυνση των υποψηφίων, πραγματοποιείται τροποποίηση ώστε ορισμένες ζητούμενες πιστοποιήσεις να ζητούνται διαζευκτικά.</p>	<p>ΝΑΙ</p>

<p>Παράγραφο 2.2.6.1</p> <p>Οι προδιαγραφές της τεχνικής ικανότητας, ως προς τα έργα, περιλαμβάνουν πολύ δεσμευτικό και ανελαστικό, κατά την άποψή μας, συνδυασμό πλήθους έργων, προϋπολογισμών και αντικειμένων. Το αποτέλεσμα είναι ότι μπορεί να διατίθεται συνολικά από τον διαγωνιζόμενο η εμπειρία, που εκτιμούμε ότι είναι το ζητούμενο, αλλά να μην είναι εφικτό αυτή να συνδυαστεί και αποτυπωθεί με τον τρόπο που απαιτείται στο τεύχος των προδιαγραφών, με αποτέλεσμα την αδυναμία συμμετοχής και συνακολούθως τη μείωση του ανταγωνισμού.</p> <p>Προτείνουμε οι απαιτήσεις επιλεξιμότητας να προσανατολιστούν στη συνάφεια των αντικειμένων και τα μεγέθη των έργων, ώστε η επιλογή προσανατολιστεί στα κύρια σημεία ενδιαφέροντος για το παρόν έργο.</p>	<p>Ζητούνται έργα που αντιστοιχούν στις πτυχές του φυσικού αντικειμένου και στο σημείο 7 της παραγράφου 2.2.6.1 έργα που συνδυάζουν πτυχές του φυσικού αντικειμένου, παρέχοντας ευελιξία στους υποψήφιους. Πραγματοποιήθηκαν αλλαγές για ακόμη μεγαλύτερη ευελιξία.</p>	<p>ΝΑΙ</p>
<p>5.1.1.</p> <p>3) Στην παράγραφο 5.1.1. αναφέρει “Η πληρωμή του αναδόχου θα πραγματοποιηθεί ως ακολούθως: Τρόπος Πληρωμής: Πραγματοποιούνται εξοφλητικές πληρωμές συγκεκριμένων παραδοτέων/φάσεων μετά την παραλαβή αυτών και την απόφαση παραλαβής της Αναθέτουσας Αρχής. Οι τμηματικές αυτές παραλαβές που οδηγούν σε αντίστοιχες πληρωμές, πραγματοποιούνται μία (1) ανά τρίμηνο.”</p> <p>Προτείνουμε να διαμορφωθεί σε : “ Η πληρωμή του αναδόχου θα πραγματοποιηθεί ως ακολούθως: Τρόπος Πληρωμής: Πραγματοποιούνται εξοφλητικές πληρωμές συγκεκριμένων παραδοτέων/φάσεων μετά την παραλαβή αυτών και την απόφαση παραλαβής της Αναθέτουσας Αρχής. Οι τμηματικές αυτές παραλαβές που οδηγούν σε αντίστοιχες πληρωμές, πραγματοποιούνται με το πέρας κάθε τμηματικής .”</p>	<p>Ο τρόπος πληρωμής που αναφέρεται στη διακήρυξη είναι συνήθης για ανάλογα έργα και το σχόλιο δεν γίνεται αποδεκτό.</p>	<p>ΟΧΙ</p>
<p>Παράγραφος 2.2.7</p> <p>2) Στην παράγραφο 2.2.7. αναφέρετε “Ισοδύναμο με τα παρακάτω Πρότυπα Διασφάλισης ποιότητας: ▪ ISO 9001:2015 για τη Διαχείριση της Ποιότητας ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 27001:2013 για την Ασφάλεια των Πληροφοριών ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 20000:2018 για την παροχή υπηρεσιών πληροφορικής ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 27701:2013 για τη Διαχείριση Προσωπικών Δεδομένων ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 29993:2017 ή άλλο ισοδύναμο εν ισχύ για την παροχή υπηρεσιών εκπαίδευσης”</p> <p>Προτείνουμε να διαμορφωθεί σε “Ισοδύναμο με τα παρακάτω Πρότυπα Διασφάλισης ποιότητας: ▪ ISO 9001:2015 για τη Διαχείριση της Ποιότητας ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 27001:2013 για την Ασφάλεια των Πληροφοριών ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 20000:2018 για την παροχή υπηρεσιών πληροφορικής ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό. ▪ ISO 27701:2013 για τη Διαχείριση Προσωπικών Δεδομένων ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό.</p>	<p>Τα Iso 22301 και 45001 κρίνονται ως σχετικά με το αντικείμενο του έργου και ενσωματώνονται στα κριτήρια επιλογής.</p> <p>Σχετικά με το ISO 29993, η διενέργεια εκπαιδεύσεων εκτός του τυπικού εκπαιδευτικού συστήματος αποτελεί μέρος του φυσικού αντικειμένου του έργου και κρίσιμη παράμετρο για την ενδυνάμωση των ΟΤΑ και κατά συνέπεια η απαίτηση παραμένει.</p>	<p>ΝΑΙ</p>

<p>ISO 45001:2018 ή άλλο ισοδύναμο εν ισχύ για την παροχή υπηρεσιών εκπαίδευσης ISO 22301:2019 ή άλλο ισοδύναμο εν ισχύ για την παροχή υπηρεσιών εκπαίδευσης</p>		
<p>Παράγραφος 2.2.6.1 Στην διακήρυξη παράγραφος 2.2.6.1 αναφέρει : “Να έχουν ολοκληρώσει επιτυχώς κατά τη διάρκεια της τελευταίας πενταετίας πριν από την καταληκτική ημερομηνία υποβολής προσφορών του παρόντος διαγωνισμού: 1. Δύο (2) έργα που να αφορούν σε σχεδιασμό και υλοποίηση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ή/και παροχής συμβουλευτικών/ μελετητικών υπηρεσιών για την εκπόνηση μελετών, πολιτικών, διαδικασιών και προτύπων ασφάλειας, ή/και Υπηρεσίες Υποστήριξης για Πιστοποίηση κατά ISO 27001:2013 2. Ένα (1) έργο που να περιλαμβάνει την παροχή υπηρεσιών, σχετικά με την αποτύπωση τρέχουσας στρατηγικής και υφιστάμενης κατάστασης πληροφοριακών συστημάτων, την ανάλυση θεσμικού περιβάλλοντος, με εστίαση στη συμμόρφωση με όλες τις προβλέψεις του θεσμικού ή/και κανονιστικού πλαισίου την πρόταση και ανάλυση αλλαγών σε οργανωτικό και επιχειρησιακό επίπεδο και την εκπόνηση προτάσεων για την ασφάλεια συστημάτων. 3. Δύο (2) έργα που να αφορούν εκπαίδευση - ευαισθητοποίηση προσωπικού στην ασφάλεια πληροφοριών, μέσω ηλεκτρονικών υπηρεσιών. 4. Δύο (2) έργα που να περιλαμβάνουν πιστοποιημένες εκπαιδεύσεις. 5. Δύο (2) έργα που να περιλαμβάνουν τη διενέργεια ελέγχων διείσδυσης (Penetration test). 6. Ένα (1) έργο που να περιλαμβάνει την προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και την εγκατάσταση του εν λόγω εξοπλισμού. 7. Έως έξι (6) έργα που έχουν συνολικό προϋπολογισμό τουλάχιστον ενός εκατομμυρίου ευρώ (1.000.000 €) και περιλαμβάνουν αθροιστικά τα κάτωθι αντικείμενα: ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) πλάνου ανάκαμψης από καταστροφή ή/και Συστήματος διαχείρισης επιχειρησιακής συνέχειας ο Διενέργεια ελέγχων παρείσδυσης (penetration test) ο Εκπόνηση μελέτης αξιολόγησης κινδύνων ο Εκπόνηση προτάσεων για την ασφάλεια συστημάτων ο Παροχή υπηρεσιών εκπαίδευσης ή/και ευαισθητοποίησης για την κυβερνοασφάλεια με χρήση πλατφόρμας εκπαίδευσης , ο Πιστοποιημένες εκπαιδεύσεις στην ασφάλεια πληροφοριών ή/και την επιχειρησιακή συνέχεια ο Προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και εγκατάσταση του εν λόγω εξοπλισμού σε τουλάχιστον τριάντα (30) σημεία με γεωγραφική διασπορά σε τουλάχιστον έξι (6) περιφέρειες. ο Υλοποίηση τουλάχιστον τριών (3) από τις παρακάτω λύσεις κυβερνοασφάλειας: ▪ Υποσύστημα SIEM με αξιοποίηση AI αλγόριθμων. ▪ Υποσύστημα δημιουργίας για honeypots. ▪ Υποσύστημα στατική ανάλυση κώδικα. ▪ Προστασία Ηλεκτρονικού Ταχυδρομείου / Secure Mail Gateway ▪ Προστασία Τελικού Σημείου”</p>	<p>Οι αλλαγές για ελάχιστο αριθμό έργων στα σημεία 1 έως 6 της παραγράφου 2.2.6.1 ενσωματώθηκαν. Η απαίτηση για μέγιστο αριθμό έργων στο σημείο 7 της παραγράφου 2.2.6.1 έχει ουσιαστικό σκοπό να διασφαλίσει ότι τα έργα που θα επικαλεστούν οι υποψήφιοι θα είναι ανάλογου μεγέθους και πολυπλοκότητας με το παρόν έργο. Για τη διευκόλυνση των υποψηφίων η απαίτηση επανακαθορίζεται σε έως οχτώ (8) έργα.</p>	<p>ΝΑΙ</p>

<p>Προτείνουμε να διαμορφωθεί ως ακολούθως με βάση την αρχή της ίσης μεταχείρισης και της μεγιστοποίησης των συμμετοχών :</p> <p>Να έχουν ολοκληρώσει επιτυχώς κατά τη διάρκεια της τελευταίας πενταετίας πριν από την καταληκτική ημερομηνία υποβολής προσφορών του παρόντος διαγωνισμού: 1. Δύο (2) έργα τουλάχιστον που αθροιστικά να αφορούν σε σχεδιασμό και υλοποίηση Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών ή/και παροχής συμβουλευτικών/ μελετητικών υπηρεσιών για την εκπόνηση μελετών, πολιτικών, διαδικασιών και προτύπων ασφάλειας, ή/και Υπηρεσίες Υποστήριξης για Πιστοποίηση κατά ISO 27001:2013 2. Ένα (1) έργο τουλάχιστον που να περιλαμβάνει την παροχή υπηρεσιών, σχετικά με την αποτύπωση τρέχουσας στρατηγικής και υφιστάμενης κατάστασης πληροφοριακών συστημάτων, την ανάλυση θεσμικού περιβάλλοντος, με εστίαση στη συμμόρφωση με όλες τις προβλέψεις του θεσμικού ή/και κανονιστικού πλαισίου την πρόταση και ανάλυση αλλαγών σε οργανωτικό και επιχειρησιακό επίπεδο και την εκπόνηση προτάσεων για την ασφάλεια συστημάτων. 3. Δύο (2) έργα τουλάχιστον που να αφορούν εκπαίδευση - ευαισθητοποίηση προσωπικού στην ασφάλεια πληροφοριών, μέσω ηλεκτρονικών υπηρεσιών. 4. Δύο (2) έργα που να περιλαμβάνουν πιστοποιημένες εκπαιδεύσεις. 5. Δύο (2) έργα που να περιλαμβάνουν τη διενέργεια ελέγχων διείσδυσης (Penetration test). 6. Ένα (1) έργο τουλάχιστον που να περιλαμβάνει την προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) ή/και την εγκατάσταση του εν λόγω εξοπλισμού. 7. Τουλάχιστον έξι (6) έργα που έχουν συνολικό προϋπολογισμό τουλάχιστον μεγαλύτερο του ενός εκατομμυρίου ευρώ (1.000.000 €) και περιλαμβάνουν αθροιστικά τα κάτωθι αντικείμενα: ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ο Σχεδιασμό ή/και συντήρηση (υποστήριξη) πλάνου ανάκαμψης από καταστροφή ή/και Συστήματος διαχείρισης επιχειρησιακής συνέχειας ο Διενέργεια ελέγχων παρείσδυσης (penetration test) ο Εκπόνηση μελέτης αξιολόγησης κινδύνων ο Εκπόνηση προτάσεων για την ασφάλεια συστημάτων ο Παροχή υπηρεσιών εκπαίδευσης ή/και ευαισθητοποίησης για την κυβερνοασφάλεια με χρήση πλατφόρμας εκπαίδευσης , ο Πιστοποιημένες εκπαιδεύσεις στην ασφάλεια πληροφοριών ή/και την επιχειρησιακή συνέχεια ο Προμήθεια εξοπλισμού ασφάλειας (τείχη προστασίας - firewalls) και εγκατάσταση του εν λόγω εξοπλισμού σε τουλάχιστον τριάντα (30) σημεία με γεωγραφική διασπορά σε τουλάχιστον έξι (6) περιφέρειες. ο Υλοποίηση τουλάχιστον τριών (3) από τις παρακάτω λύσεις κυβερνοασφάλειας: ▪ Υποσύστημα SIEM με αξιοποίηση AI αλγόριθμων. ▪ Υποσύστημα δημιουργίας για honeypots. ▪ Υποσύστημα στατική ανάλυση κώδικα. ▪ Προστασία Ηλεκτρονικού Ταχυδρομείου / Secure Mail Gateway ▪ Προστασία Τελικού Σημείου</p>		
<p>Πίνακας Συμμόρφωσης 2- Σελ 142 - Προστασία Τελικού Σημείου Η προστασία τελικού σημείου θα παρέχεται και για servers; Παρακαλούμε όπως διευκρινιστούν τα λειτουργικά συστήματα που χρησιμοποιούνται, καθώς και οι υποστηριζόμενες εκδόσεις τους.</p>	<p>Οι εν λόγω παράμετροι θα καθοριστούν κατά την υλοποίηση του έργου</p>	<p>ΟΧΙ</p>

<p>Πίνακας Συμμόρφωσης 3-Σελ 144-146 (Πλατφόρμα Κυβερνοασφάλειας) Έχοντας υπόψιν τα παρακάτω σημεία:</p> <ul style="list-style-type: none"> ο SIEM ο Υποσύστημα διαχείρισης αξιοπιστίας (TrustManagement) ο Υποσύστημα δημιουργίας honeypots ο Στατική Ανάλυση Πηγαίου Κώδικα – (SAST - Static Application Security Testing) <p>παρακαλούμε να διευκρινήσετε εάν είναι αποδεκτό να προσφερθούν λύσεις οι οποίες δύναται να ενσωματώνονται άρτια μεταξύ τους παρέχοντας ένα συνολικό σύστημα κυβερνοασφάλειας</p>	<p>Είναι αποδεκτή η προσφορά διαφορετικών λύσεων εφόσον οι υποψήφιοι τεκμηριώσουν την ικανότητά τους να λειτουργούν ως ενιαίο σύστημα και η ζητούμενη λειτουργικότητα να καλύπτεται στο σύνολό της.</p>	<p>ΟΧΙ</p>
<p>Σελ 113 Άρθρο 6- ΥΠΗΡΕΣΙΕΣ SOC Παρακαλούμε όπως διευκρινίσετε ποιο είναι το επιθυμητό SLA για αντιμετώπιση και resolution incidents; Υπάρχει ανάγκη για προσαρμοσμένα metrics, KPI ή risk scoring; Προβλέπονται SLA penalties;</p>	<p>Προστέθηκε πίνακας συμμόρφωσης με αναλυτικότερες απαιτήσεις για την υπηρεσία SOC</p>	<p>ΝΑΙ</p>
<p>2.2.6.2 - Τεχνική και Επαγγελματική Επάρκεια Α. Παρακαλούμε να διευκρινιστεί εάν είναι αποδεκτό τα στελέχη αντί του ISO27001; 2013 να κατέχουν το πιστοποιητικό ISO27001:2022 καθώς το ISO 27001:2022 αποτελεί το πλέον σύγχρονο πρότυπο "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" το οποίο ανακοινώθηκε τον Οκτώβριο 2022 με τη λογική να αντικαταστήσει πλήρως το ISO 27001:2013 σε μία τριετή μεταβατική περίοδο</p>	<p>Το ISO 27001:2022 είναι σαφώς ισοδύναμο πιστοποιητικό και είναι επαρκές για την κάλυψη των κριτηρίων επιλογής</p>	
<p>Β. Παρακαλούμε όπως διευκρινιστεί εάν με τον όρο 'ισοδύναμες' πιστοποιήσεις μπορούμε να θεωρήσουμε ότι θεωρούνται αποδεκτές οι παρακάτω πιστοποιήσεις αντί των αρχικά αναφερόμενων ανά κατηγορία :</p> <ol style="list-style-type: none"> 1. Licensed Penetration Tester (LPT) -> ισοδύναμη CEH (Certified Ethical Hacker) ή Offensive Security Certified Professional (OSCP) 2. CREST Practitioner Security Analyst (CPSA) -> ισοδύναμη CompTIA PenTest+, ή CEH (Certified Ethical Hacker) 3. CREST Certified Infrastructure Tester (CCT - INF) -> ισοδύναμη OSCP (Offensive Security Certified Professional) 4. CREST Certified Web Applications Tester (CCT - APP) -> ισοδύναμη OSWE (Offensive Security Web Expert) <p>Εναλλακτικά όπως μας υποδείξετε τις ισοδύναμες πιστοποιήσεις.</p>	<p>Παρακάτω αναφέρονται ενδεικτικές ισοδύναμες πιστοποιήσεις:</p> <ol style="list-style-type: none"> 1. Ενδεικτικές ισοδύναμες πιστοποιήσεις: Licensed Penetration Tester (LPT) -> OSEP (Offensive Security Experienced Penetration Tester). CREST Practitioner Security Analyst (CPSA) -> CompTIA PenTest+ CREST Certified Infrastructure Tester (CCT - INF) -> CSTL-INF CREST Certified Web Applications Tester (CCT - APP) -> OSWE (Offensive Security Web Expert) 2. Η LPT δεν είναι ισοδύναμη με την CEH, καθώς η CEH παρέχει κυρίως θεωρητική γνώση και βασικές δεξιότητες hacking, ενώ η LPT απαιτεί προχωρημένες πρακτικές ικανότητες, hands-on penetration testing και αυστηρή αξιολόγηση σε πραγματικά περιβάλλοντα. Σε 	<p>ΟΧΙ</p>

	<p>σχέση με την OSCP η LPT βρίσκεται σε ανώτερο επίπεδο.</p> <p>3. Η CPISA δεν είναι ισοδύναμη της CEH που παρέχει κυρίως θεωρητική γνώση και βασικές δεξιότητες hacking.</p> <p>4. Η CCT-INF δεν είναι ισοδύναμη της OSCP αφού η πρώτη επικεντρώνεται σε τεκμηριωμένη αξιολόγηση υποδομών με έμφαση στη συμμόρφωση, ενώ το OSCP επικεντρώνεται περισσότερο στη πρακτική τεχνική ικανότητα και σε hands-on testing.</p>	
<p>Γ. Παρακαλούμε όπως διευκρινιστεί για ποιόν λόγο ζητούνται υποχρεωτικές πιστοποιήσεις NCSC οι οποίες έχουν δημιουργηθεί αποκλειστικά για το περιβάλλον της Μ Βρετανίας με στόχο να συμμορφώνονται με τις οδηγίες και πολιτικές της Στρατηγικής Κυβερνοασφάλειας της Μ Βρετανίας (UK government national cyber strategy), με βάση τα παρακάτω ενδεικτικά URL links Assured CHECK Scheme Standard v1.1 NCSC Annual Review 2024, ειδικότερα μετά την έξοδο της Μ Βρετανίας από την Ε.Ε. Έχοντας υπόψη τα παραπάνω παρακαλούμε όπως διευκρινιστεί εάν θεωρούνται ως ισοδύναμες οι παρακάτω πιστοποιήσεις:</p> <p>1. NCSC CHECK Team Leader - Infrastructure (CTL - INF) -> ισοδύναμη OSCP (Offensive Security Certified Professional)</p> <ul style="list-style-type: none"> ▪ NCSC CHECK Team Leader - Web Applications (CTL - APP) -> ισοδύναμη OSWE (Offensive Security Web Expert) <p>Εναλλακτικά παρακαλούμε πολύ όπως μας υποδείξετε τις ισοδύναμες πιστοποιήσεις.</p>	<p>Οι ζητούμενες πιστοποιήσεις της NCSC ζητούνται για την έμφαση στην ηγεσία ομάδας. Η απαίτηση προσαρμόστηκε έτσι ώστε ορισμένες απαιτήσεις να ζητούνται διαζευκτικά.</p>	<p>NAI</p>
<p>6 Ασφαλής Υπηρεσία Πρόσβασης Άκρου / Secure Access Service Edge (SASE).</p> <p>Στην Προδιαγραφή 50 περιγράφονται ως μελλοντική δυνατότητα, υπηρεσίες που θα πρέπει να περιλαμβάνονται σε μία υπηρεσία SASE, καθώς εξ ορισμού αποτελούν δομικά στοιχεία της υπηρεσίας. Θα πρέπει οι απαιτήσεις αυτές να γίνουν υποχρεωτικές. Επιπροσθέτως θα πρέπει να περιληφθεί και η παροχή υπηρεσίας ασφάλειας ΖΤΝΑ, η οποία δεν αναγράφεται ως προδιαγραφή, αλλά αποτελεί βασικό στοιχείο του SASE Framework. Οι προδιαγραφές 14,15,17,19 προτείνεται να αφαιρεθούν καθώς δεν σχετίζονται άμεσα με υπηρεσία SASE. Η προδιαγραφή 20 αντιτίθεται σε θεμελιώδη λειτουργία μίας SASE υπηρεσίας και θα πρέπει να αφαιρεθεί.</p>	<p>Οι προδιαγραφές κρίνονται επαρκείς</p>	<p>OXI</p>
<p>Σχόλιο επί των Προδιαγραφών (Honeypots & SAST)</p>	<p>Είναι αποδεκτή η προσφορά διαφορετικών λύσεων εφόσον οι</p>	<p>OXI</p>

<p>Οι προδιαγραφές στις σελ. 145–146 προβλέπουν ότι οι λειτουργίες δημιουργίας honeypots και η Στατική Ανάλυση Πηγαίου Κώδικα (SAST) αποτελούν «υποσυστήματα» της πλατφόρμας κυβερνοασφάλειας/SIEM. Η απαίτηση ενσωμάτωσης αυτών των λειτουργιών ως native modules ουσιαστικά φωτογραφίζει συγκεκριμένη τεχνολογία και αποκλείει την αξιοποίηση κορυφαίων λύσεων της διεθνούς αγοράς, όπως αυτές που αξιολογούνται σε Gartner Magic Quadrants και Forrester Wave. Προτείνουμε οι σχετικές απαιτήσεις να τροποποιηθούν ώστε να είναι vendor-neutral, προβλέποντας ότι οι λειτουργίες honeypot και SAST μπορούν να παρέχονται είτε ενσωματωμένα στην πλατφόρμα είτε μέσω εξειδικευμένων 3rd-party λύσεων, με την προϋπόθεση ότι υπάρχει πλήρης και τεκμηριωμένη ολοκλήρωση με το SIEM και το SOC. Με αυτόν τον τρόπο διασφαλίζεται η απαιτούμενη λειτουργικότητα, χωρίς να περιορίζεται ο ανταγωνισμός ή να αποκλείονται ώριμες και αναγνωρισμένες τεχνολογίες της αγοράς.</p>	<p>υποψήφιοι τεκμηριώσουν την ικανότητά τους να λειτουργούν ως ενιαίο σύστημα και η ζητούμενη λειτουργικότητα να καλύπτεται στο σύνολό της.</p>	
<p>2 Αντικείμενο της Συμφωνίας Πλαίσιο Επιθυμούμε όπως διευκρινιστεί στην παράγραφο 6. Υπηρεσίες SOC (Security Operations Center): Παροχή υπηρεσιών παρακολούθησης και ανίχνευσης επιθέσεων, αν αφορούν Υπηρεσία SOCaaS (SOC as a Service) μόνο ή και περιλαμβάνουν και Υπηρεσία MDR (Managed Detection & Response).</p>	<p>Ενσωματώθηκε πίνακας συμμόρφωσης με πιο αναλυτικές απαιτήσεις για την υπηρεσία SOC.</p>	<p>ΝΑΙ</p>

Ο Διευθύνων Σύμβουλος ΕΔΥΤΕ Α.Ε.

Αριστείδης Σωτηρόπουλος