ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης

Κτηματολόγιο

Α. 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:

i. 3.1.2.1. Α.1 Identity & Access Management

Απαιτείται η προμήθεια λύσης αυτοματοποιημένης επαναφοράς forest για λόγους τακτικής άσκησης ετοιμότητας ή ανάκαμψης από κυβερνο-επίθεση, ενσωματωμένης στην πλατφόρμα λήψης αντιγράφων ασφαλείας; Να προσφερθεί η δυνατότητα ανάταξης κακόβουλων ή εσφαλμένων μεταβολών στο EntraID και Active Direcory με ένα click? Απαιτείται ενσωματωμένη δυνατότητα identity security posture;

Απάντηση:

Η λύση πρέπει να υποστηρίζει αποκατάσταση AD/forest για οποιονδήποτε από τους αναφερόμενους λόγους. Ο τρόπος παροχής της υπηρεσίας (ενσωμάτωση στην πλατφόρμα λήψης αντιγράφων ασφαλείας, stand-alone, native AD backup μέσω Windows Server Backup + Azure AD Recycle bin κ.λπ.) αποτελεί επιλογή του αναδόχου, σύμφωνα με την συνολική αρχιτεκτονική της προσφοράς του. Η δυνατότητα identity security posture δεν είναι υποχρεωτική, αλλά αναμένεται να προκύψει ως αποτέλεσμα της ολιστικής υλοποίησης Entra ID P2.

Ερώτημα 2ο:

ii. 3.1.2.2. Α.2 Προστασία Δεδομένων

Ζητείται στο πλαίσιο της διακήρυξης η δημιουργία αντιγράφων ασφαλείας των εφαρμογών M365 σε περιβάλλον air gap για λόγους ανάκαμψης από κυβερνο-επίθεση ή αστοχία χρήσης? Αν ναι, ποιος είναι ο αριθμός των mailboxes των χρηστών;

Απάντηση:

Η δημιουργία αντιγράφων σε περιβάλλον air gap δεν αποτελεί υποχρεωτική απαίτηση.

Ερώτημα 3ο

ii. 3.1.2.2. Α.2 Προστασία Δεδομένων

Απαιτείται η προστασία των endpoints (laptops, desktops) από αστοχία στη χρήση ή προσβολή από malware με δημιουργία αντιγράφων ασφαλείας με ενσωματωμένη δηνατότητα data compliance? Αν ναι, ποιος είναι ο αριθμός των χρηστών;

Απάντηση:

Ναι απαιτείται Endpoint Data Protection που καλύπτει laptops, desktops, VDI και αποτροπή διαρροής δεδομένων από endpoints. Δεν απαιτείται ξεχωριστή λύση endpoint backup με

data compliance. Στο παρόν έργο απαιτούνται κατ' ελάχιστο 2.700 χρήστες και 200 remote άδειες.

Ερώτημα 4ο

iii. 3.1.3.7. Β.2.4 Disaster recovery

Απαιτείται να προσφερθεί λύση που θα υλοποιήσει τη μεταφορά λειτουργιών στο DR Site και επαναφορά; Αν ναι: ποιος είναι ο αριθμός των VMs (εξαιρουμένων των αντιγράφων στο απομακρυσμένο κέντρο δεδομένων) ανά hypervisor? Ποιά είναι η χωρητικότητα (front end TB) των βάσεων δεδομένων Oracle και MS SQL;

Απάντηση:

Όπως αναφέρεται στην παράγραφο 3.1.3.7 απαιτείται η ανάπτυξη λεπτομερών διαδικασιών για μεταφορά λειτουργιών στο DR Site και επαναφορά. Ο αριθμός των VMs ανά hypervisor είναι περίπου 70 VMWARE, 50 HYPER-V. Η χωρητικότητα (front-end TB) των βάσεων δεδομένων MS SQL ανέρχεται σε 1 TB. Τα ανωτέρω μεγέθη θα επαληθευτούν κατά την as-is αποτύπωση στο πλαίσιο υλοποίησης του έργου καθώς και θα δοθούν περαιτέρω τεχνικές λεπτομέρειες στον Ανάδοχο μετά την ανάθεση του έργου.

Ερώτημα 5ο

iv. 3.1.4.3. Γ.3 Backup and DR Management

Για την υλοποίηση της απαίτησης της ως άνω παραγράφου της διακήρυξης, απαιτείται να προσφερθεί λύση λήψης αντιγράφων ασφαλείας? Αν ναι:

α. ποιο είναι το πλήθος των εικονικών μηχανών

β. ποια είναι η χωρητικότητα (front end TB) των βάσεων δεδομένων που λειτουργούν σε φυσικούς εξυπηρετητές;

γ. ποια είναι η χωρητικότητα (front end TB) των NAS ή file systems που λειτουργούν σε φυσικούς εξυπηρετητές;

δ. απαιτείται η δυνατότητα ελέγχου των VMs ή των file systems για πιθανή προσβολή από κακόβουλο λογισμικό και η ανάκτηση καθαρών δεδομένων;

Απάντηση:

Ναι, απαιτείται λύση λήψης αντιγράφων ασφαλείας με automated testing, immutable storage, 3-2-1 backup strategy κ.λπ., σύμφωνα με την §3.1.4.3 και §3.1.5.3. . Ο Ανάδοχος μπορεί να προσφέρει είτε out of the box λύση συγκεκριμένου κατασκευαστή, είτε να υλοποιήσει τις παραπάνω διαδικασίες στα πλαίσια του έργου.

Το πλήθος των εικονικών μηχανών είναι περίπου 70 VMWARE, 50 HYPER-V. Περισσότερες τεχνικές λεπτομέρειες θα δοθούν στον ανάδοχο με την υπογραφή της σύμβασης.

Ερώτημα 6ο

Σε συνέχεια των αναφερόμενων στην εν θέματι διακήρυξη και όσον αφορά τις σχετικές προδιαγραφές που αφορούν το DDoS Protection (on-perm) παρακαλούμε για την παροχή των ακόλουθων διευκρινίσεων :

i. Ζητείται αυτόνομο DDoS protection appliance ή καλύπτεται από άλλο deliverable (π.χ. NGFW);

ii. Σε περίπτωση αυτόνομης λύσης, ποιο είναι το απαιτούμενο Mitigation Throughput και το Packets Per Second (PPS) capacity της λύσης;

iii. Απαιτείται High Availability;

iv. Ποιος ο τύπος των network interfaces (10GbE/40GbE);

v. Ποιος ο μέγιστος αριθμός προστατευόμενων αντικειμένων (Protected Objects/IPs);

vi. Σχετικά με το integration με upstream ISP services, παρακαλούμε διευκρινίστε και κατονομάστε εάν απαιτείται Native Cloud Signaling για διασύνδεση με Cloud Scrubbing Center τρίτου παρόχου ή του ISP και ποιο το επιθυμητό μοντέλο επικοινωνίας με τον ISP;

Απάντηση:

Το DDoS Protection appliance μπορεί τεκμηριωμένα να καλύπτεται και από τον NGFW(§3.1.4.2, §3.1.2.4), τα οποία παρέχουν always-on DDoS mitigation και traffic scrubbing για το σύνολο των σημείων. Απαιτείται high availability. Τα λοιπά τεχνικά στοιχεία είναι στη διακριτική ευχέρεια του Αναδόχου ώστε να καλύπτει πλήρως τις ανάγκες του Φορέα.

Ερώτημα 7ο

Στην §3.1 «Σύνοψη του Αντικειμένου» του Παραρτήματος Ι αναφέρεται για την 1η βασική περιοχή αντικειμένου

«Α. Τεχνικές Υλοποιήσεις: Περιλαμβάνουν την εγκατάσταση, παραμετροποίηση και ενοποίηση όλων των τεχνολογικών συστημάτων ασφάλειας που απαιτούνται για την προστασία του Κτηματολογίου»

Τα ανωτέρω αναφέρονται και στην 3.1.2 «Α. ΤΕΧΝΙΚΕΣ ΥΛΟΠΟΙΗΣΕΙΣ» όπου περιγράφονται οι ζητούμενες υπηρεσίες.

Ωστόσο, στους σχετικούς με την περιοχή Α Πίνακες Συμμόρφωσης στο παράρτημα ΙΙ, ζητούνται προμήθειες αδειών. Παρακαλούμε διευκρινίστε εάν στην περιοχή αντικειμένου Α περιλαμβάνεται η προμήθεια αδειών από τον ανάδοχο.

Απάντηση:

Στο αντικείμενο Α περιλαμβάνονται η προμήθεια αδειών και οι απαραίτητες υπηρεσίες από τον Ανάδοχο για την εγκατάσταση των λύσεων (turn-key solution).

Ερώτημα 8ο

Σε συνέχεια του ανωτέρω ερωτήματος, και στην περίπτωση που απαιτείται η προμήθεια αδειών από τον Ανάδοχο:

Στον Πίνακα Συμμόρφωσης του Παραρτήματος ΙΙ και στην κατηγορία Α.1. IDM/IAM/Multi-Factor Authentication (MFA), ζητείται να προσφερθεί λύση SaaS η οποία να προσφέρεται από το Cloud για **2.700** χρήστες.

Δεδομένου ότι στην περιγραφή της αντίστοιχης υπηρεσίας (§3.1.2.1 «Α.1 Identity & Access Management» του Παρ.Ι) αναφέρεται:

«*Επέκταση Azure AD και υιοθέτηση Entra ID για την διαχείριση χρηστών και προσβάσεων*

*Το σύστημα Identity Management πρέπει να παρέχει κεντρική διαχείριση όλων των ψηφιακών ταυτοτήτων του οργανισμού (**1.900** χρήστες) , υποστηρίζοντας την ενοποίηση με το υφιστάμενο Active Directory και την επέκταση στο cloud μέσω Azure AD/Entra ID ή/και Oracle OCI (επιλογή του οργανισμού)…..»,*

Παρακαλούμε, όπως διευκρινίσετε:

α) εάν απαιτείται η επέκταση αδειών Microsoft, ποιες είναι οι υφιστάμενες άδειες του οργανισμού σχετικά με Microsoft 365;

β) Σε συνέχεια του α ανωτέρω (και εάν απαιτείται η επέκταση αδειών Microsoft), καθόσον πολλά από τα ζητούμενα συστατικά της Α περιοχής (π.χ. Entra ID P2 στην Α.1, Purview ή E5 compliance στην Α.2, Microsoft defender for endpoint P2 στην Α.3) προϋποθέτουν license Microsoft E3, πόσες τέτοιες άδειες Microsoft E3 διαθέτει ο φορέας και άρα πόσες θα πρέπει να συμπεριλάβει στην προσφορά του ο υποψήφιος;

γ) Σε συνέχεια του α ανωτέρω (και εάν απαιτείται η επέκταση αδειών Microsoft), με ποιο κανάλι σχεδιάζεται να γίνει η εν λόγω προμήθεια (Enterprise Agreement, government public cloud, άλλο);

δ) καθόσον στην §3.1.2.1 ζητούνται υπηρεσίες για 1.900 χρήστες, και στον πίνακα παραδοτέων της §3.5.2, ενώ στον Πίνακα Συμμόρφωσης ζητούνται άδειες για 2.700 χρήστες, παρακαλούμε διευκρινίστε το σωστό.

Απάντηση:

Οι υφιστάμενοι χρήστες του Φορέα είναι 1.900 αλλά προβλέπεται να αυξηθούν στους 2.700 έως την ολοκλήρωση του έργου. Οι άδειες χρήσης θα πρέπει να καλύπτουν τις μελλοντικές ανάγκες του Φορέα και συνεπώς ζητούνται 2.700 άδειες.

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). Οι αναφερόμενες άδειες EntraID και Purview αναμένεται να παρασχεθούν από το enterprise agreement της ΓΓΠΣΔΔ.

Ερώτημα 9ο

Παρακαλούμε όπως διευκρινίσετε εάν στην υποπεριοχή Α.2 «Προστασία Δεδομένων» απαιτείται προμήθεια κάποιας άδειας λογισμικού ή εάν ο φορέας διαθέτει τις απαραίτητες άδειες (π.χ. Microsoft Purview)

Απάντηση:

Επί του παρόντος ο φορέας δεν διαθέτει τις απαραίτητες άδειες Microsoft Purview. . Οι άδειες αναμένεται να παρασχεθούν στον φορέα μέσω του Enterprise Agreement ΓΓΠΣΔΔ.

Ερώτημα 10ο

Παρακαλούμε όπως διευκρινίσετε σχετικά με την υπο-περιοχή Δ.1.1 «SIEM» εάν απαιτείται διακριτά η προσφορά licenses για 3 έτη ή εάν αυτά μπορούν να ενσωματώνονται στην υπηρεσία (Γ.1.1)

Απάντηση:

Απαιτείται διακριτή τιμολόγηση των αδειών SIEM στο Μέρος Δ.1.1 της Οικονομικής Προσφοράς. Η δομή του υποδείγματος Οικονομικής Προσφοράς (Παράρτημα V) προβλέπει ξεχωριστές γραμμές για τη Δ.1.1 (Λογισμικό/Άδειες) και τη Γ.1.1 (Υπηρεσία SOC 24/7/365), και οι τιμές δεν επιτρέπεται να συμψηφίζονται μεταξύ τους

Ερώτημα 11ο

Στην §3.1.5.3 «Εξειδικευμένα Εργαλεία » του Παραρτήματος Ι ζητούνται κάποια λογισμικά, χωρίς να είναι σαφές εάν αυτά αφορούν κάποια(ες) από τις περιοχές που έχουν αναφερθεί σε προηγούμενες ενότητες (Α, Β, Γ , Δ) ή εάν είναι άλλη περιοχή.

Απάντηση:

Τα «Εξειδικευμένα Εργαλεία» της §3.1.5.3 εντάσσονται στην Περιοχή Δ (Λογισμικό και Τεχνολογικές Λύσεις) και αποτελούν αναπόσπαστο τμήμα της. Δεν συνιστούν ξεχωριστή περιοχή. Η λειτουργική τους χρήση εξυπηρετεί τις απαιτήσεις άλλων περιοχών (π.χ. Oracle Audit Vault → Α.2, Vulnerability Scanning → Β.2.5, Compliance Platform → Β.1.1, Backup & DR software → Γ.3), αλλά η προμήθεια και τιμολόγησή τους γίνεται εντός της Περιοχής Δ. Η διάθεση των απαραίτητων υπολογιστικών πόρων (VM resources) θα γίνει από την Αναθέτουσα.

Ερώτημα 12ο

Στην §3.5.2 «Παραδοτέα Σύμβασης» όπου συνοψίζονται τα παραδοτέα, παρουσιάζονται παραδοτέα Περιοχής «Εκπαίδευσης», Ε1, Ε2, Ε3 και Ε4, χωρίς να έχει περιγραφεί προηγουμένως περιοχή Ε, και χωρίς αντίστοιχη περιοχή ή υπο-περιοχή να παρατίθεται στο template Οικονομικής. Παρακαλούμε διευκρινίστε.

Απάντηση:

Τα παραδοτέα Ε.1–Ε.4 (Εκπαιδευτικό Υλικό, Εκπαιδευτικά Σεμινάρια, Helpdesk Support, Εκπαίδευση Νέων Χρηστών) δεν αποτελούν ξεχωριστή οικονομική περιοχή. Το κόστος τους

συμπεριλαμβάνεται στα αντίστοιχα Μέρη της Οικονομικής Προσφοράς στα οποία ανήκουν λειτουργικά. Η εκπαίδευση των χρηστών, η δημιουργία εκπαιδευτικού υλικού και η διοργάνωση εκπαιδευτικών σεμιναρίων έχει περιγραφεί στην Παράγραφο 3.1.6 της προκήρυξης. Το κόστος εκπαίδευσης θα πρέπει να συμπεριληφθεί στο εφάπαξ κόστος της κάθε εφαρμογής στον Πίνακα Δ.1 της οικονομικής προσφοράς.

Ερώτημα 13ο

Στην ενότητα 3.1.2.4. «Α.4 Network Security» αναφέρεται εσωτερική δικτυακής αρχιτεκτονικής 150 γεωγραφικά κατανεμημένων γραφείων. Ωστόσο, στην §3.1.1 «Υφιστάμενη Κατάσταση» 92 Κτηματολογικά Γραφεία και υποκαταστήματα, 5 κεντρικά κτίρια, 1 κτίριο στη Θεσσαλονίκη και λιγοστά σημεία αναδόχων κτηματογράφησης μέσω VPN Client. Παρακαλούμε διευκρινίστε.

Απάντηση:

Ο αριθμός 150 αποτελεί το συνολικό scope σχεδιασμού δικτυακής ασφάλειας και περιλαμβάνει τα 92 Κτηματολογικά Γραφεία και υποκαταστήματα, τα 5 κεντρικά κτίρια, το κτίριο Θεσσαλονίκης, καθώς και λοιπά σημεία πρόσβασης (σημεία αναδόχων κτηματογράφησης, απομακρυσμένη πρόσβαση VPN). Ο σχεδιασμός site-to-site VPN, NGFW deployment και network segmentation αφορά το σύνολο των 150 σημείων.

Ερώτημα 14ο

Στο Παράρτημα ΙΙ, στον πρώτο Πίνακα Συμμόρφωσης, στην προδ. Δ.2.3 ζητείται «VPN Concentrators (500 users x 80 euro per year)».

α) Παρακαλούμε όπως διευκρινίσετε ποια η απαίτηση σχετικά με τα 80 ευρώ το χρόνο.

β) Παρακαλούμε όπως διευκρινίσετε εάν οι VPN concentrators μπορούν να ταυτίζονται ως διατάξεις με τα ζητούμενα Firewalls ή πρέπει να αποτελούν ξεχωριστές συσκευές

Απάντηση:

α) Η αναφορά «x 80 euro per year» αναγράφεται εκ παραδρομής και θα πρέπει να αγνοηθεί. Η σωστή διατύπωση είναι Δ.2.3 « VPN Concentrators (500 users)»

β) Η VPN λειτουργία (SSL VPN, IPsec site-to-site) παρέχεται μέσω των κεντρικών NGFW, σύμφωνα με την §3.1.4.2. Οι VPN Concentrators δεν αποτελούν υποχρεωτικά ξεχωριστές φυσικές συσκευές·η απαίτηση δύναται να καλυφθεί από dedicated modules ή virtual instances εντός της NGFW πλατφόρμας, εφόσον πληρούνται οι λειτουργικές προδιαγραφές (500 concurrent users).

Ερώτημα 15ο

Στο παράρτημα ΙΙ, στην ενότητα για την «ΥΠΗΡΕΣΙΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ», παρατίθενται προδιαγραφές που αφορούν τον υποψήφιο. Ενδεικτικά αναφέρουμε τις κάτωθι:

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

• 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

Στην ενότητα «ΥΠΗΡΕΣΙΑ ΑΝΙΧΝΕΥΣΗΣ ΚΑΙ ΑΠΟΚΡΙΣΗΣ (MANAGED DETECTION AND RESPONSE)»

• 1.1 Η προσφερόμενη υπηρεσία να έχει υλοποιηθεί σε οργανισμούς με αντίστοιχο μέγεθος με αυτόν του κτηματολογίου

• Ο Πάροχος των υπηρεσιών θα πρέπει να έχει εκτενή εμπειρία σε EDR λύσεις. Κατ' ελάχιστο να υποστηρίζονται Microsoft Defender

Δεν είναι σαφές τι τεκμηρίωση απαιτείται και με τι ειδικούς όρους. Αρκεί η αναφορά συγκεκριμένων υλοποιήσεων ή απαιτεί βεβαιώσεις από τους αποδέκτες? Οι τυχόν βεβαιώσεις που είναι στα αγγλικά, μπορούν να θεωρούνται έγγραφα με τεχνικό περιεχόμενο που δεν απαιτούν μετάφραση καθώς καλύπτουν τεχνικές απαιτήσεις των πινάκων συμμόρφωσης? Παρακαλούμε διευκρινίστε

Απάντηση:

Για την απόδειξη εμπειρίας σε υλοποιήσεις SIEM και MDR απαιτείται βεβαίωση/δήλωση του αποδέκτη (για ιδιωτικούς φορείς) ή σχετικό αποδεικτικό έγγραφο (για δημόσιους φορείς), σύμφωνα με την §2.2.9.2 Β.4/Α2. Τυχόν υπεύθυνη δήλωση του προσφέροντος γίνεται αποδεκτή μόνο εφόσον δεν είναι δυνατή η προσκόμιση βεβαίωσης αποδέκτη, συνοδευόμενη από αντίγραφο της σχετικής σύμβασης. Βεβαιώσεις στην αγγλική γλώσσα γίνονται αποδεκτές ως έγγραφα τεχνικού περιεχομένου και δεν απαιτείται επίσημη μετάφραση.

Ερώτημα 16ο

Αναφορικά με την §3.3 του Παραρτήματος Ι, όπου ζητείται ο υποψήφιος να υποβάλει στην Προσφορά του ολοκληρωμένη πρόταση για το σχήμα διοίκησης, την οργάνωση και τον προγραμματισμό του Έργου, και το προσωπικό που θα διαθέσει για τη διοίκηση και υλοποίηση του Έργου, παρακαλούμε όπως επιβεβαιώσετε ότι δεν απαιτείται να ονοματίζονται στελέχη πέραν όσων ζητούνται στην 2.2.6, παρά μόνον ρόλοι και προφίλ.

Απάντηση:

Επιβεβαιώνεται. Στη §3.3 απαιτείται περιγραφή σχήματος διοίκησης, οργανόγραμμα και προφίλ ρόλων της ομάδας έργου. Ο ονοματισμός συγκεκριμένων στελεχών αφορά αποκλειστικά εκείνους που ορίζονται ρητά στην §2.2.6 (κριτήρια ποιοτικής επιλογής). Δεν απαιτείται επιπλέον ονοματισμός στελεχών στη §3.3.

Ερώτημα 17ο

α) Παρακαλούμε όπως διευκρινίσετε τι εννοείτε στον πίνακα Α της Οικονομικής ως «Ποσότητα» με Μονάδα Μέτρησης «Εφάπαξ». Αναμένεται η τιμή «1» στην ποσότητα;

β) Περιλαμβάνει και άδειες και α/μ υπηρεσιών;

γ) Ομοίως και για τον Β1, που αφορά αμιγώς α/μ, τι συμπληρώνεται στην ποσότητα με Μονάδα Μέτρησης «Εφάπαξ» (συμπληρώνεται η μονάδα ή η ποσότητα α/μ);.

Απάντηση:

α) Ναι, για Μονάδα Μέτρησης «Εφάπαξ» η στήλη «Ποσότητα» συμπληρώνεται με την τιμή «1». Το Σύνολο ισούται με την Τιμή Μονάδας.

β) Οι τιμές εφάπαξ στον πίνακα Α της Τεχνικής προσφοράς αφορούν το συνολικό ποσό της προσφοράς για την κάθε υπηρεσία, που περιλαμβάνει το κόστος αδειών χρήσης, υλοποίησης, εγκατάστασης και παραμετροποίησης (turn-key solution).

γ) Στο Μέρος Β.1, το οποίο αφορά αμιγώς εφάπαξ Συμβουλευτικές Υπηρεσίες, η στήλη «Ποσότητα» συμπληρώνεται επίσης με «1» (εφάπαξ αμοιβή ανά υπηρεσία), και η Τιμή Μονάδας εκφράζει το σύνολο της αμοιβής για την εκτέλεση της υπηρεσίας.

Ερώτημα 18ο

Παρακαλούμε όπως διευκρινίσετε τον Πίνακα Δ1 στην §3.1.5.1. «Δ.1 Λογισμικό Ασφάλειας» καθώς έχει σημαντικές ασάφειες. Π.χ. στα DSR Tools, έχει παραδοτέα κάθε έτος (καθόσον ζητά: Έτος-1:1 instance. Έτος-2: Βελτιώσεις UI, Έτος-3: ML υποστήριξη); Τι εννοεί ως «ML» (machine learning); Δεδομένου ότι αφορά έτοιμα λογισμικά, τι αναμένει στο Ετος-2 όπου αναφέρει «Βελτιώσεις UI»;

Απάντηση:

Η προκήρυξη δεν απαιτεί κατ' ανάγκη τη χρήση έτοιμων λογισμικών για το συγκεκριμένο. Ο Πίνακας Δ.1 για DSR Tools περιγράφει σταδιακή εξέλιξη της λύσης κατά τη διάρκεια της σύμβασης: Έτος 1: παραγωγική εγκατάσταση, Έτος 2: βελτιώσεις διεπαφής χρήστη (UI customization / tuning) βάσει λειτουργικών αναγκών του φορέα, Έτος 3: ενεργοποίηση / ενσωμάτωση δυνατοτήτων Machine Learning για αυτοματοποίηση επεξεργασίας αιτημάτων υποκειμένων δεδομένων. Το «ML» αναφέρεται σε ML-based automation features που παρέχονται από τον vendor της πλατφόρμας GDPR/DSR. Τα παραδοτέα κάθε έτους αντιστοιχούν σε ορόσημα παραλαβής, ακόμα και για ready-made λογισμικά.

Ερώτημα 19ο

Παρακαλούμε όπως διευκρινίσετε τον Πίνακα Δ2 στην §3.1.5.2. «Δ.2 Δικτυακός Εξοπλισμός» καθώς έχει σημαντικές ασάφειες. Π.χ. στα NGN Firewalls, τι αναμένει στο Ετος-2 όπου αναφέρει «+Για επέκταση»; Τι αναμένει στο Ετος-3 όπου αναφέρει «Συντήρηση licenses»; Τα licenses των firewalls σε ποιο line χρεώνονται στον πίνακα οικονομικής (Δ.2.1 NGN Firewalls ή Δ.2.2 Firewall licenses);

Απάντηση:

Ο πίνακας Δ.2 προβλέπει την επέκταση των απαιτήσεων για firewall (συσκευές και licenses) καθώς αυξάνεται ο αριθμός των χρηστών από 1.900 σε 3.000 κατά το έτος 2, και την συντήρηση / ανανέωση των licenses κατά τα έτη 2 και 3. Στο Δ.2.1 χρεώνεται το πάγιο κόστος εγκατάστασης και συντήρησης του Firewall Management Platform εφόσον υπάρχει και στο Δ.2.2. χρεώνονται τα firewall licenses.

Ερώτημα 20ο

Στον πίνακα Συμμόρφωσης υπάρχει ενότητα «Δ.2.1 - Firewall Management Platform». Σε ποιο item του πίνακα οικονομικής χρεώνεται το εν λόγω λογισμικό;

Απάντηση:

Στο Δ.2.1 χρεώνεται το πάγιο κόστος εγκατάστασης και συντήρησης του Firewall Management Platform εφόσον υπάρχει και στο Δ.2.2. χρεώνονται τα firewall licenses.

Ερώτημα 21ο

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 *A.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:

Επί του παρόντος ο φορέας δεν διαθέτει τις απαραίτητες άδειες Microsoft Purview. Οι άδειες αναμένεται να παρασχεθούν στον φορέα μέσω του Enterprise Agreement ΓΓΠΣΔΔ.

Ερώτημα 22ο

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:

Επί του παρόντος ο φορέας δεν διαθέτει τις απαραίτητες άδειες Microsoft Purview. Οι άδειες αναμένεται να παρασχεθούν στον φορέα μέσω του Enterprise Agreement ΓΓΠΣΔΔ.

Ερώτημα 23ο

Παρακαλούμε όπως επιβεβαιώσετε πως υφίσταται λύση και σχετικές άδειες λογισμικού Database Protection, 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:

Ο φορέας διαθέτει μέσω της ΓΓΠΣΔΔ μεταξύ άλλων, 45 Processors Database Enterprise Edition, μαζί με τα options:

- Advanced Security
- Audit Vault and DB Firewall
- Database Vault
- Diagnostics Pack
- Real Applications Clusters
- Tuning Pack

Ερώτημα 24ο

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:

Το κόστος ανάπτυξης της Μεθοδολογίας Αξιολόγησης και Διαχείρισης Κινδύνων θα πρέπει να συμπεριλαμβάνεται στην τιμή της πρώτης άσκησης Risk Assessment (Β.2.1) του Πίνακα Οικονομικής Β.2. Τα εν λόγω έγγραφα αποτελούν παραδοτέα που προκύπτουν στο πλαίσιο της πρώτης άσκησης, και ο Ανάδοχος δύναται να ενσωματώσει το κόστος τους στη μοναδιαία τιμή αυτής.

Ερώτημα 25ο

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:

Το κόστος ανάπτυξης των απαιτούμενων μεθοδολογιών και πλάνων θα πρέπει να συμπεριλαμβάνονται στην τιμή της πρώτης άσκησης (αντίστοιχη Β.2.x παράγραφος του Πίνακα Οικονομικής Β.2). Τα εν λόγω έγγραφα αποτελούν παραδοτέα που προκύπτουν στο πλαίσιο της πρώτης άσκησης, και ο Ανάδοχος δύναται να ενσωματώσει το κόστος τους στη μοναδιαία τιμή αυτής.

Ερώτημα 26ο

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:

Πρόκειται για δύο διακριτές απαιτήσεις:

- §3.1.3.9 (Β.2.6): Αφορά ad-hoc BC/DR drills και ασκήσεις αποκατάστασης που ζητούνται κατά διαστήματα από τον φορέα. Τιμολογούνται ανά άσκηση στον Πίνακα Β.2 και η εκτέλεσή τους εξαρτάται από τις ανάγκες του οργανισμού.
- §3.1.4.3 (Γ.3): Αφορά τακτικές Δοκιμές Disaster Recovery (quarterly testing, failover/failback validation) ως μέρος της συνεχούς υπηρεσίας Backup & DR Management. Τιμολογούνται στο Μέρος Γ (μηνιαία αμοιβή συνεχούς υπηρεσίας).

Ερώτημα 27ο

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:

Η απαίτηση ISO/IEC 27001:2022 Lead Auditor δεν καλύπτεται αυτόματα από την πιστοποίηση ISO/IEC 27001:2013 Lead Auditor, εφόσον πρόκειται για διαφορετική έκδοση του προτύπου.

Ερώτημα 28ο

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:

Η πλατφόρμα εκπαίδευσης (Δ.1.8) απαιτείται να υποστηρίζει 3.000 χρήστες, σύμφωνα με τα παραδοτέα §3.5.2 (Μέρος Δ1: Training Platform — 3.000 users). Ο αριθμός 1.900 που αναφέρεται σε άλλα σημεία αφορά αποκλειστικά τους εσωτερικούς υπαλλήλους που συμμετέχουν στα Security Awareness Training προγράμματα (§3.1.3.3 Β.1.3). Η υλική ικανότητα της πλατφόρμας πρέπει να διαστασιολογηθεί για 3.000 χρήστες.

Ερώτημα 29ο

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:

Επιβεβαιώνεται ότι η παρούσα διαγωνιστική διαδικασία δεν υποδιαιρείται σε τμήματα

Η αναφορά αφορά τις διατάξεις της παρ. 10 του άρθρου 6 του ν.4412/2016 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)» με αριθ. ΦΕΚ 147/Α/08-08-2016, όπως ισχύουν και αφορά άλλο τμήμα /διαδικασία ανάθεσης που δεν αναφέρεται στη παρούσα διακήρυξη.

Ερώτημα 30ο

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:

Επιβεβαιώνεται.

Ερώτημα 31ο

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:

Η Αναθέτουσα Αρχή, κατά το στάδιο υποβολής των προσφορών, αποδέχεται και αξιολογεί το ΕΕΕΣ όπως αυτό έχει τυποποιηθεί και αναρτηθεί στο ΕΣΗΔΗΣ. Εφόσον στο διαθέσιμο ηλεκτρονικό έντυπο του Μέρους IV είναι ενεργή προς συμπλήρωση αποκλειστικά η ενότητα «Γενική ένδειξη για όλα τα κριτήρια επιλογής», η συμπλήρωση της εν λόγω ενότητας αρκεί για την προκαταρκτική απόδειξη πλήρωσης των κριτηρίων επιλογής των § 2.2.4, 2.2.5, 2.2.6 και 2.2.7 της Διακήρυξης, σύμφωνα με το άρθρο 79 του ν. 4412/2016.

Ερώτημα 32ο

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:

Η αναφορά έχει συμπεριληφθεί εκ παραδρομής. Ο Ανάδοχος δύναται να προσφέρει συσκευές οι οποίες καλύπτουν επαρκώς το ζητούμενο firewall throughput των 17Gbps με περιθώριο επεκτασιμότητας.

Ερώτημα 33ο

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:

Η αναφορά σε VPN Concentrators δεν είναι εκ παραδρομής. Αφορά την απαίτηση παροχής SSL VPN remote access, η οποία δύναται να υλοποιηθεί είτε μέσω dedicated VPN concentrator hardware, είτε μέσω ενσωματωμένης λειτουργικότητας των NGFW, εφόσον πληρούνται οι λειτουργικές προδιαγραφές. Η επιλογή αρχιτεκτονικής εναπόκειται στον Ανάδοχο, ο οποίος οφείλει να τεκμηριώσει την εκπλήρωση της απαίτησης.

Ερώτημα 34ο

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:

Η αναφορά σε Network Monitoring Tools δεν είναι εκ παραδρομής. Αποτελεί υποχρεωτικό deliverable (§3.5.2, Μέρος Δ2: Δ.2.4) με αρχική εγκατάσταση και συντήρηση ανά έτος. Οι τεχνικές προδιαγραφές πρέπει να περιγραφούν σε ικανοποιητικό βαθμό από τον Ανάδοχο στην Τεχνική του Προσφορά. Επισημαίνεται ότι απαιτείται η προμήθεια αδειών χρήσης και εγκατάσταση των Λογισμικών από τον Ανάδοχο – η διάθεση των απαραίτητων υπολογιστικών πόρων (VM resources) θα γίνει από την Αναθέτουσα

Ερώτημα 35ο

Ποια είναι η τρέχουσα αρχιτεκτονική του Active Directory: πόσα forests/domains, αριθμός Domain Controllers, λειτουργικό επίπεδο (functional level), και υπάρχουν trust relationships με εξωτερικά domains (ΓΓΠΣ/Taxisnet);.

Απάντηση:

Τεχνικές λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 36ο

Παρακαλούμε παρέχετε: (α) πόσα Oracle 19c instances υπάρχουν (production, dev, DR); (β) σε ποια data centers φιλοξενούνται; (γ) υπάρχει υφιστάμενο Oracle Audit Vault deployment ή greenfield; (δ) χρησιμοποιούνται Oracle Exadata appliances ή standard x86;

Απάντηση:

Οι βάσεις δεδομένων του Κτηματολογίου έχουν μεταφερθεί σε Oracle Cloud Infrastructure (OCI). Περαιτέρω τεχνικές προδιαγραφές και λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 37ο

Παρακαλούμε παρέχετε πλήρες endpoint inventory: (α) Windows workstations ανά OS version (β) Windows/Linux servers (γ) POS terminals και σε ποια branches (δ) thin clients και τύπος (Citrix/VMware) (ε) mobile devices (iOS/Android) corporate-managed ή BYOD (στ) αριθμός Citrix VDI sessions;

Απάντηση:

Τεχνικές λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 38ο

Το Endpoint Security scope περιλαμβάνει laptops, VDI, POS και thin clients. Παρακαλούμε διευκρινίστε αν όλα τα ανωτέρω endpoints θεωρούνται in-scope για πλήρη EDR λειτουργικότητα (telemetry, detection, response) ή αν για ορισμένες κατηγορίες (π.χ. POS / thin clients) αναμένεται περιορισμένη λειτουργικότητα ή compensating controls.

Απάντηση:

Όλα τα παραπάνω θεωρούνται in scope. Διευκρινίζεται ότι πρέπει να υποστηρίζονται τα λειτουργικά που αναφέρονται στον Πίνακα Προδιαγραφών Α.3 "Endpoint Security" στην Προδιαγραφή 3.1.

Ερώτημα 39ο

Ο Πίνακας Συμμόρφωσης Α.4 απαιτεί υποστήριξη IBM AIX 7.x και Oracle Solaris 11.4 στο Application Microsegmentation. Ερωτάται: (α) υπάρχουν πράγματι AIX/Solaris workloads στο περιβάλλον; (β) αν ναι, πόσα και σε ποιο data center; (γ) αν όχι, επιβεβαιώνεται ότι η απαίτηση αφορά δυνητική μελλοντική επέκταση;

Απάντηση:

Ο φορέας δεν διαθέτει IBM AIX 7.x και Oracle Solaris 11.4 workloads εν λειτουργία. Η απαίτηση υποστήριξης αυτών των πλατφορμών στον Πίνακα Συμμόρφωσης Α.4 αφορά δυνητική μελλοντική επέκταση και δεν αποτελεί υποχρεωτική απαίτηση ενεργής εγκατάστασης agent για τις εν λόγω πλατφόρμες στο πλαίσιο της παρούσας σύμβασης. Ο Ανάδοχος οφείλει να δηλώσει υποστήριξη της δυνατότητας.

Ερώτημα 40ο

Σύμφωνα με τον πίνακα της σελ. 126 (1.11), η λύση οφείλει να υποστηρίζει την εγκατάσταση agent σε ευρύ σύνολο λειτουργικών συστημάτων, συμπεριλαμβανομένων Windows Server παλαιότερων εκδόσεων, Linux distributions, καθώς και πλατφορμών όπως IBM AIX 7.x (Power) και Oracle Solaris 11.4 (SPARC/x86). Παρακαλούμε επιβεβαιώστε αν για όλες τις ανωτέρω πλατφόρμες αναμένεται πλήρης ισοδυναμία EDR λειτουργιών (π.χ. endpoint isolation, automated remediation, advanced response actions), ή αν γίνονται αποδεκτές τεκμηριωμένες διαφοροποιήσεις ανά οικογένεια OS / αρχιτεκτονική, ιδίως για legacy, non-x86 ή UNIX-based λειτουργικά συστήματα.

Απάντηση:

Ο εν λόγω agent δεν επιτελει ρόλο EDR agent αλλά χρησιμοποιείται για enforcement πολιτικών σε επίπεδο applications / vms. Η προτεινόμενη πλατφόρμα πρ'επει αν υποστηρίζει application microsegmentation χαρακτηριστικά όπως αυτά περιγράφονται στον πίνακα Α.4 και θα πρέπει να υποστηρίζει εγκατάσταση στα OS που αναφέρονται στην απαίτηση 1.11.

Ερώτημα 41ο

Δεδομένου ότι τα POS terminals περιλαμβάνονται στο Endpoint Security scope, παρακαλούμε διευκρινίστε αν επιτρέπονται EDR response actions υψηλής επίδρασης (π.χ. endpoint isolation, process termination) κατά τη διάρκεια ωρών λειτουργίας, ή αν απαιτείται εναλλακτική προσέγγιση containment.

Απάντηση:

Η εκτέλεση EDR response actions υψηλής επίδρασης (π.χ. endpoint isolation, process termination) σε POS terminals κατά τις ώρες λειτουργίας δεν είναι υποχρεωτική αυτόματη ενέργεια (π.χ. ενδέχεται να απαιτείται προηγούμενη έγκριση από τον αρμόδιο φορέα). Ο Ανάδοχος οφείλει να προτείνει εναλλακτικές προσεγγίσεις containment (network isolation μέσω NAC/NGFW) για POS κατά ώρες λειτουργίας.

Ερώτημα 42ο

Η απαίτηση για application whitelisting αφορά όλα τα endpoints ή στοχευμένες κατηγορίες endpoint(π.χ. laptops, VDI); Παρακαλούμε επιβεβαιώστε αν υφίσταται εγκεκριμένο application inventory ή αν αναμένεται να δημιουργηθεί στο πλαίσιο του έργου.

Απάντηση:

Η απαίτηση application whitelisting δεν αφορά υποχρεωτικά το σύνολο των endpoints. Εφαρμόζεται κατά προτεραιότητα σε servers, POS terminals και high-risk endpoints κ.λπ. Δεν υφίσταται εγκεκριμένο application inventory· η σύνταξή του θα γίνει κατά την διάρκεια υλοποίησης του έργου.

Ερώτημα 43ο

Για την απαίτηση full disk encryption σε όλα τα endpoints, παρακαλούμε διευκρινίστε αν υπάρχει υφιστάμενη πολιτική key escrow / recovery ή αν αναμένεται να σχεδιαστεί και να υλοποιηθεί στο πλαίσιο του έργου.

Απάντηση:

Δεν υφίσταται τρέχουσα πολιτική key escrow/recovery για full disk encryption. Ο σχεδιασμός και η υλοποίηση λύσης Key Management αποτελούν ρητό παραδοτέο του έργου (§3.5.2, Α.2 — Key Management), το οποίο θα εκπονηθεί από τον Ανάδοχο στο πλαίσιο της Φάσης Α.

Ερώτημα 44ο

Παρακαλούμε διευκρινίστε ποιος φορέας (ανάδοχος, SOC, εσωτερική IT ομάδα) έχει την εξουσιοδότηση εκτέλεσης EDR response actions σε endpoints και αν υφίστανται διαφοροποιήσεις ανά κατηγορία endpoint (π.χ. user devices vs POS).

Απάντηση:

Η εξουσιοδότηση εκτέλεσης EDR response actions ορίζεται στα Response Playbooks που αναπτύσσει ο Ανάδοχος ως παραδοτέο Α.5. Κατά γενικό κανόνα: αυτόματες ενέργειες χαμηλής επίδρασης (quarantine malware, alert generation) εκτελούνται από το SOC χωρίς προηγούμενη έγκριση, ενέργειες υψηλής επίδρασης (host isolation, account suspension) εκτελούνται μετά από έγκριση εκπροσώπου της Αναθέτουσας Αρχής. Για POS terminals ενδέχεται να ισχύουν πρόσθετοι περιορισμοί κατά τις ώρες λειτουργίας

Ερώτημα 45ο

Υπάρχει ήδη τεκμηριωμένη υφιστάμενη αρχιτεκτονική δικτύου (on-premises και cloud) που θα παραδοθεί στον Ανάδοχο ή απαιτείται πλήρης αποτύπωση (as-is) και σχεδιασμός (to-be) από μηδενική βάση;

Απάντηση:

Απαιτείται πλήρης as-is αποτύπωση της υφιστάμενης δικτυακής αρχιτεκτονικής (on-premises και cloud) ως παραδοτέο Β.1.2, το οποίο ο Ανάδοχος οφείλει να εκπονήσει στην αρχή της σύμβασης. Η Αναθέτουσα Αρχή θα διαθέσει στον Ανάδοχο τα διαθέσιμα στοιχεία υποδομής, χωρίς να εγγυάται την πληρότητα της υφιστάμενης τεκμηρίωσης, η οποία θα πρέπει να συμπληρωθεί κατά την διάρκεια εκτέλεσης του έργου.

Ερώτημα 46ο

Το tender αναφέρει ταυτόχρονα «150 γεωγραφικά κατανεμημένα γραφεία», «92 Κτηματολογικά Γραφεία» και «περίπου 100 κτιριακές εγκαταστάσεις». Ερωτάται: (α) ακριβής αριθμός sites για NGFW deployment (β) τύπος WAN σύνδεσης ανά site (ADSL/VDSL/leased line/SYZEFXIS) (γ) υπάρχουν sites με 4G/5G backup μόνο;

Απάντηση:

Τα συνολικά σημεία για NGFW deployment θα είναι 150. Περαιτέρω τεχνικές προδιαγραφές και λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης (π.χ. αριθμός sites μέσω ΣΥΖΕΥΞΙΣ, ADSL/VDSL, leased line ή/και 4G/5G συνδέσεις.

Ερώτημα 47ο

Παρακαλούμε παρέχετε inventory δικτυακού εξοπλισμού: (α) κατασκευαστής/μοντέλα υπαρχόντων switches ανά site (managed/unmanaged) (β) ποιοι switches υποστηρίζουν 802.1X (γ) υπάρχουν legacy switches χωρίς VLAN tagging ή 802.1X (δ) τρέχουσα perimeter firewall λύση (κατασκευαστής, μοντέλο, throughput);

Απάντηση:

Τεχνικές λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 48ο

Το tender αναφέρει Azure μέσω ΓΓΠΣ και Oracle OCI. Ερωτάται: (α) τύπος τρέχουσας σύνδεσης ΓΓΠΣ (dedicated/SYZEFXIS/VPN) και διαθέσιμο bandwidth (β) υπάρχει ήδη Azure subscription και Oracle OCI tenancy (EU region) (γ) αναμένεται ο Ανάδοχος να προμηθεύσει ή αναβαθμίσει τη ΓΓΠΣ σύνδεση;

Απάντηση:

Τεχνικές λεπτομέρειες θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης.

Ερώτημα 49ο

Το 3.1.3.2 ορίζει ρητά ότι ZTA configuration «δεν αποτελεί αντικείμενο του παρόντος έργου», ενώ το 3.1.2.4 απαιτεί «Υλοποίηση Zero Trust Network Architecture». Ερωτάται: (α) ποιο είναι ακριβώς το ZTA scope στο Pillar A - design+configuration ή μόνο design (β) οι Conditional Access policies και network segmentation θεωρούνται ZTA configuration ή ZTA design deliverable;

Απάντηση:

Όπως αναφέρεται και στην προκήρυξη, «θα πρέπει να γίνει μια πρώτη άσκηση ανάπτυξης της target αρχιτεκτονικής, based on ZTA principles. Οποιοδήποτε configuration θα είναι συνέχεια / αποτέλεσμα της εν λόγω άσκησης και δεν αποτελεί αντικείμενο του παρόντος έργου.». Οι Conditional Access Policies και η πρόταση network segmentation θεωρούνται μέρος της στοχευόμενης αρχιτεκτονικής και άρα εμπίπτουν.

Ερώτημα 50ο

Ποιες πλατφόρμες χρησιμοποιούνται σήμερα για AD, SIEM και NAC και ποια integrations θεωρούνται υποχρεωτικά;

Απάντηση:

Υφίσταται Microsoft Active Directory. Δεν υφίσταται τρέχουσα SIEM ή NAC πλατφόρμα - πρόκειται για greenfield implementations. Περαιτέρω τεχνικές προδιαγραφές και λεπτομέρειες integration θα δοθούν στον Ανάδοχο μετά την υπογραφή της σχετικής σύμβασης και θα αποτυπωθούν στην as-is καταγραφή.

Ερώτημα 51ο

Παρακαλούμε να διευκρινιστεί αν υπάρχει διαθέσιμη εκτίμηση ή επίσημα στοιχεία σχετικά με τον συνολικό αριθμό χρηστών του οργανισμού, καθώς και διάκριση μεταξύ εσωτερικών χρηστών (internal users) και εξωτερικών χρηστών (external users, contractors, partners). Δεν αναφέρεται σχετικός αριθμός στο RFP ο οποίος είναι κρίσιμος για τον ορθό σχεδιασμό της λύσης.

Απάντηση:

Στην παράγραφο 3.1.1 της προκήρυξης αναφέρεται σαφώς το σύνολο των χρηστών και η κατανομή τους ανά κατηγορία.

Ερώτημα 52ο

Από πόσες και ποιες κατηγορίες log sources θα τροφοδοτείται το SIEM (Windows Events, Oracle Audit Vault, network Syslog/NetFlow, M365/Azure AD, WAF/IDS, application logs); Επιβεβαιώνεται ότι τα 10TB Έτους 1 αφορούν ετήσιο όγκο ingest και όχι συσσωρευτική αποθήκευση;

Απάντηση:

Οι κατηγορίες log sources περιλαμβάνουν: Windows Events (endpoints & servers), Oracle Audit Vault logs, network Syslog/NetFlow (NGFW, switches), M365/Azure AD audit logs, WAF/IDS/IPS logs, application logs κτηματολογικών εφαρμογών. Τα 10TB Έτους 1 αναφέρονται σε ετήσιο συνολικό όγκο ingest (annual ingestion volume), όχι σε συσσωρευτική αποθήκευση. Η storage capacity για retention θα διαστασιολογηθεί από τον Ανάδοχο βάσει της retention policy που θα συμφωνηθεί.

Ερώτημα 53ο

Ο Πίνακας Συμμόρφωσης 1.4 απαιτεί «κατ' ελάχιστον Microsoft Sentinel και IBM QRadar SIEM». Το IBM QRadar SaaS ανακοινώθηκε για End-of-Life τον Απρίλιο 2026. Ερωτάται: (α) αποδέχεται η Αναθέτουσα Αρχή το Azure Sentinel ως ισοδύναμο αντικατάστασης του QRadar (β) αν όχι, ποια τεκμηρίωση απαιτείται για QRadar σε 36μηνη σύμβαση όταν η πλατφόρμα θα έχει αποσυρθεί;

Απάντηση:

Ο Πίνακας Συμμόρφωσης 1.4 απαιτεί <Ο Πάροχος των υπηρεσιών θα πρέπει να έχει εκτενή εμπειρία σε περιβάλλοντα SIEM. Κατ’ ελάχιστο να υποστηρίζει Microsoft Sentinel και IBM

QRadar SIEM>. Η απαίτηση είναι ως προς την πρότερη εμπειρία του υποψήφιου αναδόχου σε εγκατάσταση και διαχείριση SIEM πλατφορμών, με το Microsoft Sentinel και IBM QRadar SIEM είναι οι 2 πιο ευρέως γνωστές και χρησιμοποιημένες πλατφόρμες στην ελληνική αγορά. Πέραν της εμπειρίας (που απαιτείται και για τις δύο πλατφόρμες όπως αναφέρεται παραπάνω) η προτεινόμενη λύση του Αναδόχου γίνεται αποδεκτό να περιλαμβάνει ως κύρια SIEM πλατφόρμα οποιαδήποτε λύση SIEM εφόσον αυτή καλύπτει τις απαιτήσεις της διακήρυξης.

Ερώτημα 54ο

Ο Πίνακας Συμμόρφωσης απαιτεί «φυσική παρουσία ομάδας απόκρισης στις εγκαταστάσεις Κτηματολογίου στην Αττική εντός 4 ωρών για κρίσιμα περιστατικά». Ερωτάται: (α) ισχύει η υποχρέωση 24/7/365 συμπεριλαμβανομένων αργιών και νυκτερινών ωρών (β) ποιες εγκαταστάσεις in-scope (μόνο Μεσογείων ή και Ασπρόπυργος) (γ) υπάρχει ανώτατος αριθμός κρίσιμων περιστατικών ανά έτος;

Απάντηση:

(α) ναι αφορά 24/7/365

(β) αφορά όλες τις εγκαταστάσεις των κεντρικών κτιρίων του Κτηματολογίου στην Αττική

(γ) δεν προβλέπεται ανώτατος αριθμός κρίσιμων περιστατικών

Ερώτημα 55ο

Ο Πίνακας Συμμόρφωσης 3.3–3.7 απαιτεί AI Agentic service με GPT-4o, GPT-4 Turbo, Gemini 1 Pro/1.5 Pro. Ερωτάται: (α) τα LLM endpoints πρέπει να βρίσκονται αποκλειστικά σε EU regions ή αρκεί GDPR-compliant DPA με US-hosted endpoints (β) η απαίτηση RAG+MCP αφορά native SIEM integration ή αρκεί API integration μέσω middleware;

Απάντηση:

(α) δεν είναι απαραίτητο τα LLM endpoints να είναι εντός ΕΕ αρκεί να συμμορφώνονται πλήρως με τη σχετική Ευρωπαϊκη και Ελληνική νομοθεσία και το κανονιστικό πλαίσιο GDPR

(β) Η RAG+MCP integration δύναται να υλοποιηθεί μέσω API integration με middleware, χωρίς να απαιτείται native SIEM integration. Η προτεινόμενη επιλογή τεχνικής λύσης θα πρέπει να τεκμηριωθεί από τον Ανάδοχο στα πλαίσια της Τεχνικής Προσφοράς.

Ερώτημα 56ο

Το 3.5.3 ορίζει ότι «οι υπηρεσίες Γ παρέχονται συνεχώς από την έναρξη του έργου». Ωστόσο το Μέρος Α (SIEM setup, NGFW, endpoint rollout) εκτελείται τους πρώτους 6 μήνες. Ερωτάται: (α) το SOC 24/7 ξεκινά από ημέρα 1 ή από ολοκλήρωση Μέρους Α (Μ6) (β) αν ημέρα 1, ποιες SOC υπηρεσίες παρέχονται πριν ολοκλήρωση SIEM (γ) υπάρχουν ήδη log sources άμεσα ενσωματώσιμοι;

Απάντηση:

(α) Οι υπηρεσίες υποστήριξης και λειτουργίας θα προσφέρονται από την έναρξη του έργου ανάλογα με τις ανάγκες του Φορέα και τις δυνατότητες υλοποίησης. Σύμφωνα με §3.5.3, οι υπηρεσίες Γ παρέχονται συνεχώς από την έναρξη του έργου. Το SOC 24/7 ξεκινά από ημέρα 1.

(β) Πριν ολοκλήρωση SIEM), το SOC παρέχει monitoring με βάση διαθέσιμους log sources (Windows Event Logs, AD audit, NGFW logs), incident triage και response, χωρίς πλήρες SIEM correlation. Η υπηρεσία λειτουργεί σε «interim mode» έως την ολοκλήρωση SIEM deployment.

(γ) Ναι, log sources άμεσα ενσωματώσιμοι: Windows Security Event Logs, Active Directory logs, network device syslog.

Αναμένουμε αναλυτικό προτεινόμενο χρονοδιάγραμμα από τον Ανάδοχο ανάλογα με την εμπειρία του.

Ερώτημα 57ο

Ο Πίνακας Δ.2 περιλαμβάνει «NGN Firewalls (2 νέες συσκευές) + Firewall Licenses + VPN Concentrators + Network Monitoring Tools» αλλά δεν αναφέρει branch εξοπλισμό. Επιβεβαιώνεται: (α) ο branch δικτυακός εξοπλισμός (switches, routers) ΔΕΝ εντάσσεται στο Δ.2 (β) η NGFW function στα branches παρέχεται από τα 2 κεντρικά NGFW μέσω SD-WAN ή software (γ) υπάρχει hardware refresh στα branches;

Απάντηση:

α) Επιβεβαιώνεται. Ο branch δικτυακός εξοπλισμός (switches, routers) δεν εντάσσεται στο Δ.2 και δεν αποτελεί αντικείμενο προμήθειας στο πλαίσιο της παρούσας σύμβασης.

β) Επιβεβαιώνεται. Η NGFW λειτουργία στα 150 σημεία παρέχεται από τα 2 κεντρικά NGFW, σύμφωνα με την §3.1.4.2.

γ) Hardware refresh στα branches δεν αποτελεί αντικείμενο της παρούσας σύμβασης.

Ερώτημα 58ο

Ο 2 «Σκοπός» αναφέρει «ανάπτυξη νέου DR Site», ενώ το 3.1.3.9 ορίζει ρητά «δεν περιλαμβάνεται η ανάπτυξη νέου DR site». Ερωτάται: (α) υπάρχει ήδη DR Site και σε ποια τοποθεσία (β) αν όχι, η ανάπτυξη νέου DR site εντάσσεται σε αυτή τη σύμβαση ή επόμενο project (γ) ο Ανάδοχος θα σχεδιάσει architecture DR site (design only) ή θα εφαρμόσει DR procedures επί υφιστάμενης υποδομής;

Απάντηση:

Το έργο δεν περιλαμβάνει την ανάπτυξη νέου DR Site. Ο Ανάδοχος καλείται να αναπτύξει λεπτομερείς διαδικασίες για τη μεταφορά των κρίσιμων λειτουργιών του οργανισμού στο Disaster Recovery Site σε περίπτωση καταστροφής ή σημαντικού συμβάντος που καθιστά το κύριο site μη λειτουργικό, και να εκτελέσει δοκιμές αποκατάστασης και drills στην υφιστάμενη υποδομή DR Site.

Ερώτημα 59ο

Στον τομέα παροχής υπηρεσιών SOCaaS (Γ.1.1), ο κυρίαρχος τρόπος τιμολόγησης στην αγορά των διαχειριζόμενων υπηρεσιών ασφάλειας (MSSP) είναι το μοντέλο «embedded licensing», στο οποίο οι άδειες λειτουργίας της πλατφόρμας SIEM (Δ.1.1) και της πλατφόρμας Threat Intelligence (Δ.1.7) αποτελούν αναπόσπαστο τμήμα της μηνιαίας αμοιβής για την παροχή της SOCaaS υπηρεσίας, χωρίς να τιμολογούνται ξεχωριστά ως ανεξάρτητες άδειες λογισμικού. Ερωτάται: (α) Γίνεται δεκτή η προσφορά μοντέλου SOCaaS στο οποίο το κόστος των αδειών SIEM (Δ.1.1) και Threat Intelligence Platform (Δ.1.7) ενσωματώνεται πλήρως στη μηνιαία τιμή της υπηρεσίας Γ.1.1 (SOC 24/7/365), με αποτέλεσμα οι αντίστοιχες γραμμές Δ.1.1 και Δ.1.7 στον Πίνακα Τιμολόγησης Μέρους Δ.1 να αναγράφουν μηδενικό κόστος (€0), συνοδευόμενες από τεκμηρίωση ότι η αξία αυτή περιλαμβάνεται στην Γ.1.1; (β) Σε περίπτωση που το ανωτέρω μοντέλο γίνεται δεκτό, επιβεβαιώνεται ότι η αξία των ενσωματωμένων αδειών δεν θα προσμετράται στο cap του Μέρους Δ.1 (€2.370.500) αλλά στο cap του Μέρους Γ (€4.063.200), εφόσον τιμολογείται ως μέρος της μηνιαίας αμοιβής λειτουργίας; (γ) Εάν το μοντέλο embedded licensing δεν γίνεται δεκτό, παρακαλούμε να διευκρινιστεί εάν είναι αποδεκτό εναλλακτικά το μοντέλο «consumption-based licensing» - δηλαδή η τιμολόγηση των αδειών SIEM βάσει πραγματικού όγκου ingest (GB/ημέρα ή TB/μήνα) αντί σταθερής ετήσιας άδειας - και εάν ο Πίνακας Δ.1 μπορεί να αντικατοπτρίζει εκτιμώμενο μηνιαίο κόστος κατανάλωσης αντί σταθερής τιμής. Αναφορά Διακήρυξης: Οικονομικό Αντικείμενο Μέρος Δ.1 (σελ. 163–164), 3.1.4.1 Γ.1 SOC 24/7/365 (σελ. 93–94), Πίνακας Συμμόρφωσης 1.4 και 6.5 (σελ. 108–110).

Απάντηση:

Η οικονομική προσφορά θα πρέπει να ακολουθεί τους πίνακες της προκήρυξης χωρίς απόκλιση για λόγους συγκρισιμότητας και πληρότητας των στοιχείων. Σε περίπτωση ενιαίας τιμολόγησης θα πρέπει ο Ανάδοχος να κάνει την κατανομή μεταξύ κόστους υπηρεσίας και κόστους αδειών και να συμπληρώσει όλους τους πίνακες της Οικονομικής Προσφοράς με τα αντίστοιχα δεδομένα.

Consumption-based licensing δεν γίνεται αποδεκτό. Απαιτείται σταθερή ετήσια τιμολόγηση αδειών ανά γραμμή του Πίνακα Δ.1, ώστε να είναι δυνατή η σύγκριση προσφορών.

Ερώτημα 60ο

Ο Πίνακας Λογισμικού Ασφάλειας (3.1.5.1) ορίζει τα volumetrics για το SIEM ως εξής: Έτος 1 — 1.500 endpoints / 10TB logs, Έτος 2 — +500 endpoints / +5TB logs, Έτος 3 — «Επέκταση κάλυψης». Προκειμένου οι προσφέροντες να δύνανται να προσδιορίσουν με ακρίβεια την αρχιτεκτονική, την τιμολόγηση και τις τεχνικές προδιαγραφές της SIEM πλατφόρμας, ζητούνται οι ακόλουθες διευκρινίσεις: (α) Ορισμός «TB logs»: Το μέγεθος 10TB Έτους 1 και +5TB Έτους 2 αναφέρεται σε: (i) συνολικό ετήσιο όγκο δεδομένων που ingest-άρονται στο SIEM (annual ingestion volume), (ii) ημερήσιο μέσο όγκο ingest (GB/ημέρα), ή (iii) συνολική απαιτούμενη χωρητικότητα αποθήκευσης (storage capacity) για το χρονικό διάστημα που ορίζει η πολιτική retention; Η διαφορά μεταξύ των ανωτέρω ερμηνειών επιδρά σημαντικά στη διαστασιολόγηση και κοστολόγηση της λύσης. (β) Retention Policy: Ποια είναι η απαιτούμενη πολιτική διατήρησης logs (retention period) για το SIEM; Ειδικότερα: πόσοι μήνες «hot» storage (άμεσα αναζητήσιμα δεδομένα) και πόσοι μήνες «cold/archive» storage απαιτούνται; Η retention policy επηρεάζει καθοριστικά τη συνολική χωρητικότητα

αποθήκευσης που πρέπει να τιμολογηθεί. (γ) Πηγές logs (Log Sources): Τα αναφερόμενα TB καλύπτουν αποκλειστικά on-premises log sources (Windows Events, Oracle Audit Vault, network devices, endpoints) ή περιλαμβάνουν και logs από cloud περιβάλλοντα (Microsoft Azure/M365 audit logs μέσω ΓΓΠΣ, Oracle OCI logs); Σε περίπτωση που τα cloud logs δεν περιλαμβάνονται, ποιος είναι ο εκτιμώμενος επιπλέον όγκος που θα προκύψει από αυτές τις πηγές; (δ) Έτος 3 — «Επέκταση κάλυψης»: Η διατύπωση «Επέκταση κάλυψης» για το Έτος 3 δεν συνοδεύεται από ποσοτικά στοιχεία. Παρακαλούμε διευκρινίστε: (i) ποιος είναι ο αναμενόμενος αριθμός νέων endpoints/συστημάτων που θα ενταχθούν στο Έτος 3 και (ii) ποιος ο αντίστοιχος εκτιμώμενος όγκος logs — ή, εναλλακτικά, επιβεβαιώνεται ότι η τιμολόγηση του Έτους 3 υπολογίζεται βάσει της εκτίμησης του Αναδόχου, χωρίς δεσμευτική ποσοτική απαίτηση εκ μέρους της Αναθέτουσας Αρχής; (ε) Μέτρηση endpoints: Η καταμέτρηση «1.500 endpoints» αναφέρεται σε: (i) αριθμό φυσικών/εικονικών μηχανών με εγκατεστημένο SIEM agent (MDE/AMA), (ii) αριθμό ενεργών χρηστών που παράγουν events, ή (iii) συνολικό αριθμό monitored assets (συμπεριλαμβανομένων network devices, servers, OT/IoT);

Απάντηση:

α) Τα αναφερόμενα TB (Έτος 1: 10TB, Έτος 2: +5TB) αντιστοιχούν σε ετήσιο συνολικό όγκο δεδομένων ingest (annual ingestion volume). Δεν αναφέρονται σε ημερήσιο μέσο όρο ή συνολική storage capacity.

β) Η απαιτούμενη retention policy είναι: 3 μήνες «hot» storage (άμεσα αναζητήσιμα δεδομένα) και 21 μήνες «cold/archive» storage. Ο Ανάδοχος θα διαστασιολογήσει την αποθηκευτική ικανότητα αντίστοιχα.

γ) Τα αναφερόμενα TB καλύπτουν τόσο on-premises log sources (Windows Events, Oracle Audit Vault, network devices, endpoints) όσο και cloud περιβάλλοντα (Microsoft Azure/M365 audit logs, Oracle OCI logs).

δ) Για το Έτος 3, ο Ανάδοχος δύναται να διαστασιολογήσει βάσει σταθερής ετήσιας αύξησης

ε) Οι «1.500 endpoints» αναφέρονται στον αριθμό managed assets (φυσικά/εικονικά συστήματα) με εγκατεστημένο SIEM agent (MDE / Azure Monitor Agent), συμπεριλαμβανομένων servers, workstations και network devices.

Ερώτημα 61ο

Θα πρέπει να υπάρχει απευθείας διασύνδεση με εφαρμογές για provisioning χρηστών; αν ναι με ποιες εφαρμογές;

Απάντηση:

Ναι, απαιτείται user provisioning integration με τις κύριες εφαρμογές του φορέα. Κατ' ελάχιστον, η λύση IAM πρέπει να υποστηρίζει automated provisioning/deprovisioning για: Active Directory, Azure AD/Entra ID, Microsoft 365 (Exchange, SharePoint, Teams), κτηματολογικές εφαρμογές (Oracle-based). Ο πλήρης κατάλογος εφαρμογών και οι μέθοδοι ενσωμάτωσης θα προσδιοριστούν κατά την as-is αποτύπωση (παραδοτέο Β.1.2).

Ερώτημα 62ο

Παρακαλείσθε να αναφέρετε τον αριθμό και τους τύπους των συστημάτων που αποτελούν έγκυρη πηγή πληροφοριών σχετικά με τις παραμέτρους ταυτότητας για integration με την προτεινομένη λύση (παραδείγματα παραμέτρων: όνομα, επώνυμο, προϊστάμενος, είδος απασχόλησης, ημερομηνία έναρξης και λήξης της σύμβασης, τμήμα) π.χ. Σύστημα ανθρώπινου δυναμικού, τόσο ως πηγή για τους υπαλλήλους όσο και ως εξωτερικές ταυτότητες.

Απάντηση:

Πρωτεύον authoritative source για όλους τους χρήστες είναι το υφιστάμενο Active Directory. Δευτερεύοντα συστήματα που ενδέχεται να αποτελούν πηγή identity parameters (π.χ. σύστημα διαχείρισης ανθρωπίνου δυναμικού / μισθοδοσία, εξωτερικά directories συνεργατών) θα αποτυπωθούν κατά την as-is ανάλυση. Δεν υφίσταται ξεχωριστό HR / HCM σύστημα που να αποτελεί επίσημη authoritative πηγή εκτός AD.

Ερώτημα 63ο

Ποιες λύσεις διαχείρισης ταυτότητας, χρηστών και πρόσβασης (IAM, IGA, PAM, AD, MFA, SSO) χρησιμοποιούνται σήμερα από την υπηρεσία;

Απάντηση:

Τρέχουσες λύσεις: Microsoft Active Directory (on-premises). Δεν υφίστανται υφιστάμενες λύσεις IGA, PAM, MFA ή SSO. Δεν υφίσταται υφιστάμενο Entra ID / Azure AD deployment. Όλες οι προβλεπόμενες λύσεις IAM αποτελούν greenfield implementations στο πλαίσιο της παρούσας σύμβασης.

Ερώτημα 64ο

Ποια και πόσα συστήματα/εφαρμογές θα ληφθούν υπόψη για ενοποίηση με το IAM (συστήματα/εφαρμογές στα οποία τα δικαιώματα/δικαιώματα πρόσβασης των χρηστών πρέπει να διαχειρίζονται από τη λύση IAM):
α. τη λειτουργία τους,
β. πεδίο εφαρμογής,
γ. τρέχουσα προσέγγιση της διαχείρισης δικαιωμάτων,
δ. την τεχνολογία με την οποία δημιουργήθηκαν,
ε. πιθανές μέθοδοι ενσωμάτωσης,
στ. αριθμός συμβάντων που σχετίζονται με τη χορήγηση/τροποποίηση/ανάκληση αδειών που λαμβάνουν χώρα σε κάθε σύστημα κατά τη διάρκεια ενός μήνα

Απάντηση:

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

Ερώτημα 65ο

Ποια είναι η τρέχουσα αρχιτεκτονική του Active Directory: πόσα forests/domains, αριθμός Domain Controllers, λειτουργικό επίπεδο (functional level), και υπάρχουν trust relationships με εξωτερικά domains (ΓΓΠΣ/Taxisnet);

Απάντηση:

Βλέπε Ερώτημα 35.

Ερώτημα 66ο

Παρακαλούμε παρέχετε κατάλογο εφαρμογών που απαιτούν SSO integration: (α) πόσες χρησιμοποιούν SAML 2.0/OAuth 2.0 έναντι legacy/ιδιόκτητων πρωτοκόλλων; (β) υπάρχουν εφαρμογές που απαιτούν LDAP pass-through ή form-based auth; (γ) περιλαμβάνονται RDS WebAccess και Oracle PeopleSoft;

Απάντηση:

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

Ερώτημα 67ο

a)Πόσα είναι τα endpoints (laptops, desktops, VDI) που πρέπει να καλυφθούν; b)Πόσοι είναι οι χρήστες M365 (Exchange, SharePoint, OneDrive, Teams); c)Υπάρχουν non-Microsoft workloads (π.χ. τρίτα mail gateways, on-prem file shares) που πρέπει να ενταχθούν στο scope;

Απάντηση:

α) Ο συνολικός αριθμός endpoints in-scope (laptops, desktops, VDI) περίπου 1.700.

β) Ο αριθμός χρηστών Microsoft 365 είναι 1.700 χρήστες και αναμένεται να αυξηθούν σε 2.700.

γ) Ναι, υπάρχουν non-Microsoft workloads που εντάσσονται στο scope: Oracle 19c database servers, Linux servers. Ο πλήρης κατάλογος θα προσδιοριστεί κατά την as-is αποτύπωση.

Ερώτημα 68ο

Στην **παρ. 2.2.9.2 Αποδεικτικά μέσα - Δικαιολογητικά προσωρινού αναδόχου σημείο Β.4/Α2** της Διακήρυξης μεταξύ άλλων αναφέρεται: «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 όπως επιβεβαιώσετε ότι για την απόδειξη της ορθής ολοκλήρωσης των έργων ιδιωτικών φορέων αρκεί μόνη η υποβολή βεβαίωσης / δήλωσης του αποδέκτη με την οποία θα συμπεραίνεται η άρτια και εντός του χρονοδιαγράμματος υλοποίηση του έργου, η ημερομηνία ολοκλήρωσής του, το αντικείμενο της υπηρεσίας και το τελικό

καταβληθέν οικονομικό τίμημα, χωρίς αυτή να συνοδεύεται από αντίγραφο της σχετικής σύμβασης.

Απάντηση:

Επιβεβαιώνεται. Η προσκόμιση αντιγράφου σχετικής σύμβασης δύναται να απαιτηθεί από τον φορέα εφόσον από την βεβαίωση δεν συνάγεται ακριβώς το αντικείμενο του έργου που έχει εκτελεστεί.

Ερώτημα 69ο

Σχετικά με την προδιαγραφή 2.3 του πίνακα Δ.2.2 – FIREWALLS, παρακαλούμε να διευκρινιστεί εάν η ζήτηση για 25G θύρες είναι εκ παραδρομής καθώς το ζητούμενο firewall throughput είναι 17Gbps και κατ' επέκταση δεν προκύπτει τεχνικός λόγος για χρήση πορτών 25Gbps.

Απάντηση:

Βλέπε Ερώτημα 32.

Η Γενική Διευθύντρια
OLYMPIA MARKELLOU
16.07.2026 15:28

Ολυμπία Μαρκέλλου