Δημόσια Διαβούλευση

(Περιγραφή Φυσικού και Οικονομικού Αντικειμένου, Δικαίωμα Συμμετοχής, Κριτήρια Ποιοτικής Επιλογής και Ανάθεσης)

για το Έργο

«Προμήθεια εξοπλισμού, λογισμικού και παροχή υπηρεσιών ενίσχυσης της ασφάλειας του δικτύου δεδομένων της ΜΟΔ Α.Ε.»

Κωδικοί CPV:

32420000-3 (Εξοπλισμός δικτύου)

48732000-8 (Πακέτα λογισμικού ασφάλειας δεδομένων)

72246000-1 (Υπηρεσίες παροχής συμβουλών σε θέματα συστημάτων πληροφορικής)

72253200-5 (Υπηρεσίες υποστήριξης συστημάτων πληροφορικής)

με εκτιμώμενη αξία 3.463.000 Ευρώ (με ΦΠΑ)

Αναθέτουσα Αρχή: Μονάδα Οργάνωσης της Διαχείρισης Αναπτυξιακών Προγραμμάτων (ΜΟΔ) Α.Ε.

Διαδικασία Ανάθεσης: Ανοικτός Διεθνής Διαγωνισμός άνω των ορίων, με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομική άποψη προσφορά, βάσει βέλτιστης σχέσης ποιότητας - τιμής

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2021-2027

Περιεχόμενα

1. Συνοπτική Περιγραφή φυσικού και οικονομικού αντικειμένου της σύμβασης

Αντικείμενο της σύμβασης αποτελεί η προμήθεια εξοπλισμού και λογισμικού ενίσχυσης της ασφάλειας του δικτύου δεδομένων της ΜΟΔ Α.Ε., που αναλύεται περαιτέρω σε:

1. **Προμήθεια δύο (2) συσκευών Next Generation Firewall (NGF)**
2. **Προμήθεια Web Application Firewall με την μορφή virtual appliance (WAF)**
3. **Προμήθεια δύο (2) Virtual appliances για την προστασία των χρηστών κατά την περιήγηση στο διαδίκτυο (Web Proxy)**
4. **Προμήθεια virtual appliance για την ενιαία διαχείριση των συσκευών NGF, WAF και Web Proxy**
5. **Προμήθεια λογισμικού δημιουργίας αντιγράφων ασφάλειας και αποκατάστασης καταστροφών για 500 εικονικούς εξυπηρετητές**
6. **Προμήθεια λογισμικού Διαχείρισης Προνομιακών Προσβάσεων (Privileged Access Management – PAM).**
7. **Προμήθεια Λογισμικού Ανάλυσης και Παρακολούθησης Δικτύου**
8. **Προμήθεια Λογισμικού Asset Management**
9. **Πλατφόρμα περιορισμού Ransomware**
10. **Επέκταση χρονικής διάρκειας αδειών χρήσης του υφιστάμενου εξοπλισμού (Fortigate 601E, fortimail, fortianalyzer) της Αναθέτουσας Αρχής, ώστε να συμπίπτουν με τις υπό προμήθεια άδειες χρήσης των προϊόντων που αναφέρονται στα σημεία 1 έως 4.**

Το σύνολο του παραπάνω εξοπλισμού και λογισμικών συνοδεύεται από υπηρεσίες επανασχεδιασμού της υφιστάμενης αρχιτεκτονικής και των ζωνών ασφαλείας του δικτύου δεδομένων, υπηρεσίες εγκατάστασης και εκπαίδευσης, καθώς και:

1. **Υπηρεσίες καθημερινής υποστήριξης για χρονικό διάστημα τριών (3) ετών, από τουλάχιστον δύο (2) άτομα στην διαχείριση συσκευών και λογισμικών ασφάλειας δικτύου και συστημάτων πληροφορικής.**
2. **Υπηρεσίες Ανίχνευσης και Αποτίμησης Ευπαθειών οι οποίες θα περιλαμβάνουν έλεγχο διείσδυσης στο εξωτερικό και εσωτερικό περιβάλλον των υποδομών.**
3. **Υπηρεσίες Παρακολούθησης και Διαχείρισης της Ασφάλειας του Δικτύου Δεδομένων 24 x 7 για χρονικό διάστημα τριών (3) ετών, από Security Operation Center το οποίο θα είναι εγκατεστημένο εντός Ελλάδος.**
4. **Υπηρεσίες Παραμετροποίησης Εξοπλισμού & Λογισμικού**

Τα προς προμήθεια είδη κατατάσσονται στους ακόλουθους κωδικούς του Κοινού Λεξιλογίου δημοσίων συμβάσεων (CPV): 32420000-3 (Εξοπλισμός δικτύου), 48732000-8 (Πακέτα λογισμικού ασφάλειας δεδομένων).

Οι παρεχόμενες υπηρεσίες κατατάσσονται στους ακόλουθους κωδικούς του Κοινού Λεξιλογίου δημοσίων συμβάσεων (CPV): 72246000-1 (Υπηρεσίες παροχής συμβουλών σε θέματα συστημάτων πληροφορικής), 72253200-5 (Υπηρεσίες υποστήριξης συστημάτων πληροφορικής).

Ως **μεικτή σύμβαση**, περιλαμβάνουσα προμήθειες και υπηρεσίες, βάσει της εκτιμώμενης αξίας των προμηθειών και υπηρεσιών αντιστοίχως και σύμφωνα με το άρθρο 4 του ν. 4412/2016, η παρούσα σύμβαση **καθορίζεται ως σύμβαση υπηρεσιών**.

Η παρούσα σύμβαση δεν υποδιαιρείται σε τμήματα.

Η εκτιμώμενη αξία της σύμβασης ανέρχεται στο ποσό των τριών εκατομμυρίων τετρακοσίων εξήντα τριών ευρώ (3.463.000€) συμπεριλαμβανομένου ΦΠΑ 24%.

Η διάρκεια της σύμβασης **ορίζεται σε τρία (3) έτη από την υπογραφής της.**

Η σύμβαση θα ανατεθεί με το κριτήριο της πλέον συμφέρουσας από οικονομική άποψη προσφοράς, βάσει της βέλτιστης σχέσης ποιότητας – τιμής.

2. Δικαίωμα Συμμετοχής - Κριτήρια Ποιοτικής Επιλογής

2.1 Δικαίωμα συμμετοχής

1. Δικαίωμα συμμετοχής στη διαδικασία σύναψης της παρούσας σύμβασης έχουν φυσικά ή νομικά πρόσωπα και, σε περίπτωση ενώσεων οικονομικών φορέων, τα μέλη αυτών, που είναι εγκατεστημένα σε:

α) κράτος-μέλος της Ένωσης,

β) κράτος-μέλος του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.),

γ) τρίτες χώρες που έχουν υπογράψει και κυρώσει τη ΣΔΣ, στο βαθμό που η υπό ανάθεση δημόσια σύμβαση καλύπτεται από τα Παραρτήματα 1, 2, 4, 5, 6 και 7 και τις γενικές σημειώσεις του σχετικού με την Ένωση Προσαρτήματος Ι της ως άνω Συμφωνίας, καθώς και

δ) σε τρίτες χώρες που δεν εμπίπτουν στην περίπτωση γ΄ της παρούσας παραγράφου και έχουν συνάψει διμερείς ή πολυμερείς συμφωνίες με την Ένωση σε θέματα διαδικασιών ανάθεσης δημοσίων συμβάσεων.

Στο βαθμό που καλύπτονται από τα Παραρτήματα 1, 2, 4, 5 6 και 7 και τις γενικές σημειώσεις του σχετικού με την Ένωση Προσαρτήματος Ι της ΣΔΣ, καθώς και τις λοιπές διεθνείς συμφωνίες από τις οποίες δεσμεύεται η Ένωση, οι αναθέτουσες αρχές επιφυλάσσουν για τα έργα, τα αγαθά, τις υπηρεσίες και τους οικονομικούς φορείς των χωρών που έχουν υπογράψει τις εν λόγω συμφωνίες μεταχείριση εξίσου ευνοϊκή με αυτήν που επιφυλάσσουν για τα έργα, τα αγαθά, τις υπηρεσίες και τους οικονομικούς φορείς της Ένωσης.

2. Οικονομικός φορέας συμμετέχει είτε μεμονωμένα είτε ως μέλος ένωσης. Οι ενώσεις οικονομικών φορέων, συμπεριλαμβανομένων και των προσωρινών συμπράξεων, δεν απαιτείται να περιβληθούν συγκεκριμένη νομική μορφή για την υποβολή προσφοράς. Η αναθέτουσα αρχή μπορεί να απαιτήσει από τις ενώσεις οικονομικών φορέων να περιβληθούν συγκεκριμένη νομική μορφή, εφόσον τους ανατεθεί η σύμβαση.

Στις περιπτώσεις υποβολής προσφοράς από ένωση οικονομικών φορέων, όλα τα μέλη της ευθύνονται έναντι της αναθέτουσας αρχής αλληλέγγυα και εις ολόκληρον.

3. Η ένωση που υποβάλλει κοινή προσφορά πρέπει απαραίτητα να προσδιορίζει την έκταση, το είδος συμμετοχής κάθε μέλους της, συμπεριλαμβανομένης της κατανομής της αμοιβής μεταξύ τους, τον συντονιστή/εκπρόσωπό της ένωσης και να συμπληρώσει αντίστοιχα στην περίπτωση αυτή τα σχετικά πεδία του ΕΕΕΣ σύμφωνα με την παρ. 2.4.1. της παρούσης.

2.2 Εγγύηση συμμετοχής

2.2.1. Για την έγκυρη συμμετοχή στη διαδικασία σύναψης της παρούσας σύμβασης, κατατίθεται από τους συμμετέχοντες οικονομικούς φορείς (προσφέροντες), εγγυητική επιστολή συμμετοχής, ποσού **πενήντα πέντε χιλιάδων οκτακοσίων πενήντα τεσσάρων ευρώ (€ 55.854,00)**.

Στην περίπτωση ένωσης οικονομικών φορέων, η εγγύηση συμμετοχής περιλαμβάνει και τον όρο ότι η εγγύηση καλύπτει τις υποχρεώσεις όλων των οικονομικών φορέων που συμμετέχουν στην ένωση.

Η εγγύηση συμμετοχής πρέπει να ισχύει τουλάχιστον για **τριάντα (30) ημέρες μετά τη λήξη του χρόνου ισχύος της προσφοράς**, άλλως η προσφορά απορρίπτεται. Η αναθέτουσα αρχή μπορεί, πριν τη λήξη της

προσφοράς, να ζητά από τους προσφέροντες να παρατείνουν, πριν τη λήξη τους, τη διάρκεια ισχύος της προσφοράς και της εγγύησης συμμετοχής.

Οι πρωτότυπες εγγυήσεις συμμετοχής, πλην των εγγυήσεων που εκδίδονται ηλεκτρονικά, προσκομίζονται, σε κλειστό φάκελο με ευθύνη του οικονομικού φορέα, το αργότερο πριν την ημερομηνία και ώρα αποσφράγισης των προσφορών, άλλως η προσφορά απορρίπτεται ως απαράδεκτη, μετά από γνώμη της Επιτροπής Διαγωνισμού.

2.2.2. Η εγγύηση συμμετοχής επιστρέφεται στον ανάδοχο με την προσκόμιση της εγγύησης καλής εκτέλεσης.

Η εγγύηση συμμετοχής επιστρέφεται στους λοιπούς προσφέροντες, σύμφωνα με τα ειδικότερα οριζόμενα στην παρ. 3 του άρθρου 72 του ν. 4412/2016.

2.2.3. Η εγγύηση συμμετοχής καταπίπτει, εάν ο προσφέρων:

α) αποσύρει την προσφορά του κατά τη διάρκεια ισχύος αυτής,

β) παρέχει, εν γνώσει του, ψευδή στοιχεία ή πληροφορίες,

γ) δεν προσκομίσει εγκαίρως τα προβλεπόμενα δικαιολογητικά κατακύρωσης,

δ) δεν προσέλθει εγκαίρως για υπογραφή του συμφωνητικού,

ε) υποβάλει μη κατάλληλη προσφορά, με την έννοια της περ. 46 της παρ. 1 του άρθρου 2 του ν. 4412/2016,

στ) δεν ανταποκριθεί στη σχετική πρόσκληση της αναθέτουσας αρχής να εξηγήσει την τιμή ή το κόστος της προσφοράς του εντός της τεθείσας προθεσμίας και η προσφορά του απορριφθεί,

ζ) στις περιπτώσεις των παρ. 3, 4 και 5 του άρθρου 103 του ν. 4412/2016, περί πρόσκλησης για υποβολή δικαιολογητικών από τον προσωρινό ανάδοχο, αν, κατά τον έλεγχο των παραπάνω δικαιολογητικών, διαπιστωθεί ότι τα στοιχεία που δηλώθηκαν στο ΕΕΕΣ είναι εκ προθέσεως απατηλά, ή ότι έχουν υποβληθεί πλαστά αποδεικτικά στοιχεία, ή αν, από τα παραπάνω δικαιολογητικά που προσκομίσθηκαν νομίμως και εμπροθέσμως, δεν αποδεικνύεται η μη συνδρομή των λόγων αποκλεισμού ή η πλήρωση μιας ή περισσότερων από τις απαιτήσεις των κριτηρίων ποιοτικής επιλογής.

2.3 Λόγοι αποκλεισμού

Αποκλείεται από τη συμμετοχή στην παρούσα διαδικασία σύναψης σύμβασης (διαγωνισμό) οικονομικός φορέας, εφόσον συντρέχει στο πρόσωπό του (εάν πρόκειται για μεμονωμένο φυσικό ή νομικό πρόσωπο) ή σε ένα από τα μέλη του (εάν πρόκειται για ένωση οικονομικών φορέων) ένας ή περισσότεροι από τους ακόλουθους λόγους:

2.3.1. Όταν υπάρχει σε βάρος του αμετάκλητη καταδικαστική απόφαση για ένα από τα ακόλουθα εγκλήματα:

α) Συμμετοχή σε εγκληματική οργάνωση, όπως αυτή ορίζεται στο άρθρο 2 της απόφασης-πλαίσιο 2008/841/ΔΕΥ του Συμβουλίου της 24ης Οκτωβρίου 2008, για την καταπολέμηση του οργανωμένου εγκλήματος (ΕΕ L 300 της 11.11.2008 σ.42), και τα εγκλήματα του άρθρου 187 του Ποινικού Κώδικα (εγκληματική οργάνωση).

β) Ενεργητική δωροδοκία, όπως ορίζεται στο άρθρο 3 της σύμβασης περί της καταπολέμησης της διαφθοράς στην οποία ενέχονται υπάλληλοι των Ευρωπαϊκών Κοινοτήτων ή των κρατών-μελών της Ένωσης (ΕΕ C 195 της 25.6.1997, σ. 1) και στην παρ. 1 του άρθρου 2 της απόφασης-πλαίσιο 2003/568/ΔΕΥ του Συμβουλίου της 22ας Ιουλίου 2003, για την καταπολέμηση της δωροδοκίας στον ιδιωτικό τομέα (ΕΕ L 192 της 31.7.2003, σ. 54), καθώς και όπως ορίζεται στο εθνικό δίκαιο του οικονομικού φορέα, και τα εγκλήματα των άρθρων 159Α (δωροδοκία πολιτικών προσώπων), 236 (δωροδοκία υπαλλήλου), 237 παρ. 2-4

(δωροδοκία δικαστικών λειτουργών), 237Α παρ. 2 (εμπορία επιρροής – μεσάζοντες), 396 παρ. 2 (δωροδοκία στον ιδιωτικό τομέα) του Ποινικού Κώδικα.

γ) Απάτη εις βάρος των οικονομικών συμφερόντων της Ένωσης, κατά την έννοια των άρθρων 3 και 4 της Οδηγίας (ΕΕ) 2017/1371 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2017 σχετικά με την καταπολέμηση, μέσω του ποινικού δικαίου, της απάτης εις βάρος των οικονομικών συμφερόντων της Ένωσης (L 198/28.07.2017) και τα εγκλήματα των άρθρων 159Α (δωροδοκία πολιτικών προσώπων), 216 (πλαστογραφία), 236 (δωροδοκία υπαλλήλου), 237 παρ. 2-4 (δωροδοκία δικαστικών λειτουργών), 242 (ψευδής βεβαίωση, νόθευση κ.λπ.) 374 (διακεκριμένη κλοπή), 375 (υπεξαίρεση), 386 (απάτη), 386Α (απάτη με υπολογιστή), 386Β (απάτη σχετική με τις επιχορηγήσεις), 390 (απιστία) του Ποινικού Κώδικα και των άρθρων 155 επ. του Εθνικού Τελωνειακού Κώδικα (ν. 2960/2001, Α' 265), όταν αυτά στρέφονται κατά των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης ή συνδέονται με την προσβολή αυτών των συμφερόντων, καθώς και τα εγκλήματα των άρθρων 23 (διασυνοριακή απάτη σχετικά με τον ΦΠΑ) και 24 (επικουρικές διατάξεις για την ποινική προστασία των οικονομικών συμφερόντων της Ευρωπαϊκής Ένωσης) του ν. 4689/2020 (Α' 103).

δ) Τρομοκρατικά εγκλήματα ή εγκλήματα συνδεόμενα με τρομοκρατικές δραστηριότητες, όπως ορίζονται, αντιστοίχως, στα άρθρα 3-4 και 5-12 της Οδηγίας (ΕΕ) 2017/541 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2017 για την καταπολέμηση της τρομοκρατίας και την αντικατάσταση της απόφασης-πλαισίου 2002/475/ΔΕΥ του Συμβουλίου και για την τροποποίηση της απόφασης 2005/671/ΔΕΥ του Συμβουλίου (ΕΕ L 88/31.03.2017) ή ηθική αυτουργία ή συνέργεια ή απόπειρα διάπραξης εγκλήματος, όπως ορίζονται στο άρθρο 14 αυτής, και τα εγκλήματα των άρθρων 187Α και 187Β του Ποινικού Κώδικα, καθώς και τα εγκλήματα των άρθρων 32-35 του ν. 4689/2020 (Α'103).

ε) Νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή χρηματοδότηση της τρομοκρατίας, όπως αυτές ορίζονται στο άρθρο 1 της Οδηγίας (ΕΕ) 2015/849 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ης Μαΐου 2015, σχετικά με την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από παράνομες δραστηριότητες ή για τη χρηματοδότηση της τρομοκρατίας, την τροποποίηση του κανονισμού (ΕΕ) αριθμ. 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, και την κατάργηση της οδηγίας 2005/60/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και της οδηγίας 2006/70/ΕΚ της Επιτροπής (ΕΕ L 141/05.06.2015) και τα εγκλήματα των άρθρων 2 και 39 του ν. 4557/2018 (Α' 139).

στ) Παιδική εργασία και άλλες μορφές εμπορίας ανθρώπων, όπως ορίζονται στο άρθρο 2 της Οδηγίας 2011/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Απριλίου 2011, για την πρόληψη και την καταπολέμηση της εμπορίας ανθρώπων και για την προστασία των θυμάτων της, καθώς και για την αντικατάσταση της απόφασης-πλαίσιο 2002/629/ΔΕΥ του Συμβουλίου (ΕΕ L 101 της 15.4.2011, σ. 1), και τα εγκλήματα του άρθρου 323Α του Ποινικού Κώδικα (εμπορία ανθρώπων).

Ο οικονομικός φορέας αποκλείεται, επίσης, όταν το πρόσωπο εις βάρος του οποίου εκδόθηκε αμετάκλητη καταδικαστική απόφαση είναι μέλος του διοικητικού, διευθυντικού ή εποπτικού οργάνου του ή έχει εξουσία εκπροσώπησης, λήψης αποφάσεων ή ελέγχου σε αυτό. Η υποχρέωση του προηγούμενου εδαφίου αφορά:

- στις περιπτώσεις εταιρειών περιορισμένης ευθύνης (Ε.Π.Ε.) ιδιωτικών κεφαλαιουχικών εταιρειών (Ι.Κ.Ε.) και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.) τους διαχειριστές,

- στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον διευθύνοντα Σύμβουλο, τα μέλη του Διοικητικού Συμβουλίου, καθώς και τα πρόσωπα στα οποία με απόφαση του Διοικητικού Συμβουλίου έχει ανατεθεί το σύνολο της διαχείρισης και εκπροσώπησης της εταιρείας,

- στις περιπτώσεις Συνεταιρισμών, τα μέλη του Διοικητικού Συμβουλίου,

- σε όλες τις υπόλοιπες περιπτώσεις νομικών προσώπων, τον κατά περίπτωση νόμιμο εκπρόσωπο.

Εάν στις ως άνω περιπτώσεις (α) έως (στ) η κατά τα ανωτέρω περίοδος αποκλεισμού δεν έχει καθοριστεί με αμετάκλητη απόφαση, αυτή ανέρχεται σε πέντε (5) έτη από την ημερομηνία της καταδίκης με αμετάκλητη απόφαση.

2.3.2. Στις ακόλουθες περιπτώσεις:

α) όταν ο οικονομικός φορέας έχει αθετήσει τις υποχρεώσεις του όσον αφορά στην καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης και αυτό έχει διαπιστωθεί από δικαστική ή διοικητική απόφαση με τελεσίδικη και δεσμευτική ισχύ, σύμφωνα με διατάξεις της χώρας όπου είναι εγκατεστημένος ή την εθνική νομοθεσία ή

β) όταν η αναθέτουσα αρχή μπορεί να αποδείξει με τα κατάλληλα μέσα ότι ο οικονομικός φορέας έχει αθετήσει τις υποχρεώσεις του όσον αφορά την καταβολή φόρων ή εισφορών κοινωνικής ασφάλισης.

Αν ο οικονομικός φορέας είναι Έλληνας πολίτης ή έχει την εγκατάστασή του στην Ελλάδα, οι υποχρεώσεις του που αφορούν τις εισφορές κοινωνικής ασφάλισης καλύπτουν τόσο την κύρια όσο και την επικουρική ασφάλιση.

Οι υποχρεώσεις των ανωτέρω περ. α' και β' θεωρείται ότι δεν έχουν αθετηθεί εφόσον δεν έχουν καταστεί ληξιπρόθεσμες ή εφόσον αυτές έχουν υπαχθεί σε δεσμευτικό διακανονισμό που τηρείται.

Δεν αποκλείεται ο οικονομικός φορέας, όταν έχει εκπληρώσει τις υποχρεώσεις του είτε καταβάλλοντας τους φόρους ή τις εισφορές κοινωνικής ασφάλισης που οφείλει, συμπεριλαμβανομένων, κατά περίπτωση, των δεδουλευμένων τόκων ή των προστίμων είτε υπαγόμενος σε δεσμευτικό διακανονισμό για την καταβολή τους στο μέτρο που τηρεί τους όρους του δεσμευτικού κανονισμού.

2.3.3. Αποκλείεται από τη συμμετοχή στη διαδικασία σύναψης της παρούσας σύμβασης, οικονομικός φορέας σε οποιαδήποτε από τις ακόλουθες καταστάσεις:

(α) Εάν έχει αθετήσει τις υποχρεώσεις που προβλέπονται στην παρ. 2 του άρθρου 18 του ν. 4412/2016, περί αρχών που εφαρμόζονται στις διαδικασίες σύναψης δημοσίων συμβάσεων.

(β) Εάν τελεί υπό πτώχευση ή έχει υπαχθεί σε διαδικασία ειδικής εκκαθάρισης ή τελεί υπό αναγκαστική διαχείριση από εκκαθαριστή ή από το δικαστήριο ή έχει υπαχθεί σε διαδικασία πτωχευτικού συμβιβασμού ή έχει αναστείλει τις επιχειρηματικές του δραστηριότητες ή έχει υπαχθεί σε διαδικασία εξυγίανσης και δεν τηρεί τους όρους αυτής ή εάν βρίσκεται σε οποιαδήποτε ανάλογη κατάσταση προκύπτουσα από παρόμοια διαδικασία, προβλεπόμενη σε εθνικές διατάξεις νόμου. Η αναθέτουσα αρχή μπορεί να μην αποκλείει έναν οικονομικό φορέα ο οποίος βρίσκεται σε μία εκ των καταστάσεων που αναφέρονται στην περίπτωση αυτή, υπό την προϋπόθεση ότι αποδεικνύει ότι ο εν λόγω φορέας είναι σε θέση να εκτελέσει τη σύμβαση, λαμβάνοντας υπόψη τις ισχύουσες διατάξεις και τα μέτρα για τη συνέχιση της επιχειρηματικής του λειτουργίας.

(γ) Εάν, με την επιφύλαξη της παραγράφου 3β του άρθρου 44 του ν. 3959/2011 περί ποινικών κυρώσεων και άλλων διοικητικών συνεπειών, υπάρχουν επαρκώς εύλογες ενδείξεις που οδηγούν στο συμπέρασμα ότι ο οικονομικός φορέας συνήψε συμφωνίες με άλλους οικονομικούς φορείς με στόχο τη στρέβλωση του ανταγωνισμού.

δ) Εάν μία κατάσταση σύγκρουσης συμφερόντων κατά την έννοια του άρθρου 24 του ν. 4412/2016 δεν μπορεί να θεραπευθεί αποτελεσματικά με άλλα, λιγότερο παρεμβατικά, μέσα.

(ε) Εάν μία κατάσταση στρέβλωσης του ανταγωνισμού από την πρότερη συμμετοχή του οικονομικού φορέα κατά την προετοιμασία της διαδικασίας σύναψης σύμβασης, σύμφωνα με όσα ορίζονται στο άρθρο 48 του ν. 4412/2016, δεν μπορεί να θεραπευθεί με άλλα, λιγότερο παρεμβατικά, μέσα.

(στ) Εάν έχει επιδείξει σοβαρή ή επαναλαμβανόμενη πλημμέλεια κατά την εκτέλεση ουσιώδους απαίτησης στο πλαίσιο προηγούμενης δημόσιας σύμβασης, προηγούμενης σύμβασης με αναθέτοντα φορέα ή

προηγούμενης σύμβασης παραχώρησης που είχε ως αποτέλεσμα την πρόωρη καταγγελία της προηγούμενης σύμβασης, αποζημιώσεις ή άλλες παρόμοιες κυρώσεις.

(ζ) Εάν έχει κριθεί ένοχος εκ προθέσεως σοβαρών απατηλών δηλώσεων κατά την παροχή των πληροφοριών που απαιτούνται για την εξακρίβωση της απουσίας των λόγων αποκλεισμού ή την πλήρωση των κριτηρίων επιλογής, έχει αποκρύψει τις πληροφορίες αυτές ή δεν είναι σε θέση να προσκομίσει τα δικαιολογητικά κατακύρωσης.

(η) Εάν επιχείρησε να επηρεάσει με αθέμιτο τρόπο τη διαδικασία λήψης αποφάσεων της αναθέτουσας αρχής, να αποκτήσει εμπιστευτικές πληροφορίες που ενδέχεται να του αποφέρουν αθέμιτο πλεονέκτημα στη διαδικασία σύναψης σύμβασης ή να παράσχει με απατηλό τρόπο παραπλανητικές πληροφορίες που ενδέχεται να επηρεάσουν ουσιωδώς τις αποφάσεις που αφορούν τον αποκλεισμό, την επιλογή ή την ανάθεση.

(θ) Εάν η αναθέτουσα αρχή μπορεί να αποδείξει, με κατάλληλα μέσα ότι έχει διαπράξει σοβαρό επαγγελματικό παράπτωμα, το οποίο θέτει εν αμφιβόλω την ακεραιότητά του.

Εάν στις ως άνω περιπτώσεις (α) έως (θ) η περίοδος αποκλεισμού δεν έχει καθοριστεί με αμετάκλητη απόφαση, αυτή ανέρχεται σε τρία (3) έτη από την ημερομηνία έκδοσης πράξης που βεβαιώνει το σχετικό γεγονός.

Κυρώσεις των άρθρων 206, 207, 208, 213, 218, 219 και 220 του ν. 4412/2016, συνολικού ύψους που δεν ξεπερνά τις δύο εκατοστιαίες μονάδες (2%), επί της αξίας της σύμβασης στο πλαίσιο της οποίας επιβλήθηκαν για την πλημμελή εκτέλεση απαίτησης σε οικονομικό φορέα δεν θεωρούνται σοβαρή πλημμέλεια για την εφαρμογή της περ. (στ) της παρ. 4 του άρθρου 73, εφόσον ο οικονομικός φορέας έχει εξοφλήσει το σύνολο του ποσού στην αναθέτουσα αρχή., εκτός αν η αναθέτουσα αρχή κρίνει διαφορετικά.

Η δε παράλειψη της δήλωσης των παραπάνω κυρώσεων στο Ευρωπαϊκό Ενιαίο Έγγραφο Σύμβασης δεν λαμβάνεται υπόψη για την εφαρμογή της περ. ζ΄ του άρθρου 73 του ν. 4412/2016.

Για τον υπολογισμό των δύο εκατοστιαίων μονάδων (2%) του πρώτου εδαφίου δεν υπολογίζονται οι κυρώσεις για τις οποίες τα επανορθωτικά μέτρα που έλαβαν οι οικονομικοί φορείς έχουν κριθεί επαρκή από την αρμόδια Επιτροπή της παρ. 9 του άρθρου 73 του ν. 4412/2016.

2.3.4 Αποκλείεται, επίσης, οικονομικός φορέας από τη συμμετοχή στη διαδικασία σύναψης της παρούσας σύμβασης εάν συντρέχουν οι προϋποθέσεις εφαρμογής της παρ. 4 του άρθρου 8 του ν. 3310/2005, όπως ισχύει (αμιγώς εθνικός λόγος αποκλεισμού). Οι υποχρεώσεις της παρούσης αφορούν τις ανώνυμες εταιρείες που υποβάλλουν προσφορά αυτοτελώς ή ως μέλη ένωσης ή που συμμετέχουν στο μετοχικό κεφάλαιο άλλου νομικού προσώπου που υποβάλλει προσφορά ή νομικά πρόσωπα της αλλοδαπής που αντιστοιχούν σε ανώνυμη εταιρεία.

Εξαιρούνται της υποχρέωσης αυτής:

α) οι εισηγμένες στα χρηματιστήρια κρατών-μελών της Ευρωπαϊκής Ένωσης ή του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) εταιρείες,

β) οι εταιρείες, τα δικαιώματα ψήφου των οποίων ελέγχονται από μία ή περισσότερες επιχειρήσεις επενδύσεων (investment firms), εταιρείες διαχείρισης κεφαλαίων/ενεργητικού (asset/fund managers) ή εταιρείες διαχείρισης κεφαλαίων επιχειρηματικών συμμετοχών (private equity firms), υπό την προϋπόθεση ότι οι τελευταίες αυτές εταιρείες ελέγχουν, συνολικά ποσοστό που υπερβαίνει το εβδομήντα πέντε τοις εκατό (75%) των δικαιωμάτων ψήφων και είναι εποπτευόμενες από Επιτροπές Κεφαλαιαγοράς ή άλλες αρμόδιες χρηματοοικονομικές αρχές κρατών μελών της Ευρωπαϊκής Ένωσης ή του Ο.Ο.Σ.Α.

2.3.4.α. Απαγορεύεται η ανάθεση της παρούσας σύμβασης, σε:

α) Ρώσο υπήκοο ή φυσικό ή νομικό πρόσωπο, οντότητα ή φορέα που έχει την έδρα του στη Ρωσία,

β) νομικό πρόσωπο, οντότητα ή φορέα του οποίου τα δικαιώματα ιδιοκτησίας κατέχει άμεσα ή έμμεσα σε ποσοστό άνω του 50% οντότητα αναφερόμενη στο στοιχείο α) της παρούσας παραγράφου,˙ ή

γ) φυσικό ή νομικό πρόσωπο, οντότητα ή φορέα που ενεργεί εξ ονόματος ή κατ' εντολή οντότητας αναφερόμενης στο στοιχείο α) ή β) της παρούσας παραγράφου, συμπεριλαμβανομένων, όταν αντιστοιχούν σε περισσότερο από το 10% της αξίας της σύμβασης, των υπεργολάβων, προμηθευτών ή οντοτήτων (τρίτων) στις ικανότητες των οποίων στηρίζεται, κατά την έννοια των οδηγιών για τις δημόσιες συμβάσεις.

2.3.5. Ο οικονομικός φορέας αποκλείεται σε οποιοδήποτε χρονικό σημείο κατά τη διάρκεια της διαδικασίας σύναψης της παρούσας σύμβασης, όταν αποδεικνύεται ότι βρίσκεται, λόγω πράξεων ή παραλείψεών του, είτε πριν είτε κατά τη διαδικασία, σε μία από τις ως άνω περιπτώσεις.

2.3.6. Οικονομικός φορέας που εμπίπτει σε μια από τις καταστάσεις που αναφέρονται στις παραγράφους 2.3.1 και 2.3.3, εκτός από την περ. β αυτής, μπορεί να προσκομίζει στοιχεία, προκειμένου να αποδείξει ότι τα μέτρα που έλαβε επαρκούν για να αποδείξουν την αξιοπιστία του, παρότι συντρέχει ο σχετικός λόγος αποκλεισμού (αυτοκάθαρση). Για τον σκοπό αυτόν, ο οικονομικός φορέας αποδεικνύει ότι έχει καταβάλει ή έχει δεσμευθεί να καταβάλει αποζημίωση για ζημίες που προκλήθηκαν από το ποινικό αδίκημα ή το παράπτωμα, ότι έχει διευκρινίσει τα γεγονότα και τις περιστάσεις με ολοκληρωμένο τρόπο, μέσω ενεργού συνεργασίας με τις ερευνητικές αρχές, και έχει λάβει συγκεκριμένα τεχνικά και οργανωτικά μέτρα, καθώς και μέτρα σε επίπεδο προσωπικού κατάλληλα για την αποφυγή περαιτέρω ποινικών αδικημάτων ή παραπτωμάτων. Τα μέτρα που λαμβάνονται από τους οικονομικούς φορείς αξιολογούνται σε συνάρτηση με τη σοβαρότητα και τις ιδιαίτερες περιστάσεις του ποινικού αδικήματος ή του παραπτώματος. Εάν τα στοιχεία κριθούν επαρκή, ο εν λόγω οικονομικός φορέας δεν αποκλείεται από τη διαδικασία σύναψης σύμβασης. Αν τα μέτρα κριθούν ανεπαρκή, γνωστοποιείται στον οικονομικό φορέα το σκεπτικό της απόφασης αυτής. Οικονομικός φορέας που έχει αποκλειστεί, σύμφωνα με τις κείμενες διατάξεις, με τελεσίδικη απόφαση, σε εθνικό επίπεδο, από τη συμμετοχή σε διαδικασίες σύναψης σύμβασης ή ανάθεσης παραχώρησης δεν μπορεί να κάνει χρήση της ανωτέρω δυνατότητας κατά την περίοδο του αποκλεισμού που ορίζεται στην εν λόγω απόφαση.

2.3.7. Η απόφαση για την διαπίστωση της επάρκειας ή μη των επανορθωτικών μέτρων κατά την προηγούμενη παράγραφο εκδίδεται σύμφωνα με τα οριζόμενα στις παρ. 8 και 9 του άρθρου 73 του ν.4412/2016. Η απόφαση για τη διαπίστωση της επάρκειας ή μη των επανορθωτικών μέτρων κατά την προηγούμενη παράγραφο, εκδίδεται σύμφωνα με τα οριζόμενα στις παρ. 8 και 9 του άρθρου 73 του ν.4412/2016, καθώς και στην υπ' αριθμ. 102080/24-10-2022 (Β΄5623/02.11.2022) απόφαση του Υπουργού Ανάπτυξης και Επενδύσεων με θέμα «Ρύθμιση θεμάτων σχετικά με την εξέταση επανορθωτικών μέτρων από την Επιτροπή της παρ. 9 του άρθρου 73 του ν. 4412/2016».

Η αναθέτουσα αρχή αποστέλλει στη Γνωμοδοτική Επιτροπή Εξέτασης Μέτρων Αυτοκάθαρσης για Δημόσιες Συμβάσεις Προμηθειών και Υπηρεσιών, η οποία συγκροτήθηκε με την αρ. 71973/18.09.2025 απόφαση του Υπουργού Ανάπτυξης (ΑΔΑ: 6ΥΟ446ΝΛΣΞ-ΙΨΖ) το σχέδιο της απόφασής της περί της διαπίστωσης της επάρκειας ή μη των ληφθέντων από τον οικονομικό φορέα επανορθωτικών μέτρων, συνοδευόμενο από πλήρη φάκελο που περιλαμβάνει όλα τα σχετικά με την υπόθεση στοιχεία. Το σχέδιο της απόφασης της αναθέτουσας αρχής, μαζί με όλα τα σχετικά με την υπόθεση στοιχεία αποστέλλονται, ηλεκτρονικά στη διεύθυνση ηλεκτρονικού ταχυδρομείου epanorthotika-prom-yp@eaadhsy.gr.

Στην περίπτωση που ο οικονομικός φορέας δεν έχει προσκομίσει, με δική του πρωτοβουλία, τα στοιχεία, με τα οποία αποδεικνύονται τα επικαλούμενα μέτρα αυτοκάθαρσης (εκδοθείσες αποφάσεις διοίκησης, αποδεικτικά εξόφλησης προστίμων, αλληλογραφία με αρμόδιες ελεγκτικές αρχές κ.λπ.), η αναθέτουσα αρχή, πριν από τη σύνταξη και αποστολή του σχεδίου απόφασης στην Επιτροπή, υποχρεούται να ζητήσει από τον οικονομικό φορέα την προσκόμισή τους, εντός προθεσμίας που δεν υπερβαίνει τις δέκα (10) ημέρες. Με την παρέλευση της ανωτέρω προθεσμίας, θεωρείται ότι τα αιτούμενα στοιχεία δεν

προσκομίστηκαν. Στην περίπτωση που ο οικονομικός φορέας υποβάλει αίτημα για παράταση της ως άνω προθεσμίας, συνοδευόμενο από έγγραφα, με τα οποία αποδεικνύεται ότι έχει αιτηθεί τη χορήγηση των στοιχείων, η αναθέτουσα αρχή παρατείνει την προθεσμία υποβολής, για όσο χρόνο απαιτηθεί για τη χορήγησή τους από τις αρμόδιες δημόσιες αρχές.

Αν η αναθέτουσα αρχή κρίνει ότι τα στοιχεία που προσκόμισε ο οικονομικός φορέας δεν είναι πλήρη ή απαιτούνται διευκρινίσεις, πριν από την αποστολή του σχεδίου της απόφασής της στην Επιτροπή, καλεί τον οικονομικό φορέα για τη συμπλήρωση των σχετικών στοιχείων ή/και την παροχή διευκρινίσεων, εντός προθεσμίας, που δεν υπερβαίνει τις δέκα (10) ημέρες.

Αν ο οικονομικός φορέας δεν ανταποκριθεί στην πρόσκληση της αναθέτουσας αρχής, το γεγονός αυτό μνημονεύεται στο σχέδιο της απόφασης.

Με την επιφύλαξη της επόμενης παραγράφου, δεν εξετάζονται από την Επιτροπή επανορθωτικά μέτρα που επικαλείται ένας οικονομικός φορέας, προκειμένου να αποδείξει την αξιοπιστία του, εφόσον αυτά έχουν ληφθεί **μετά** την ημερομηνία λήξης υποβολής των προσφορών. Στην περίπτωση αυτή, η αναθέτουσα αρχή δεν τα λαμβάνει υπόψη και δεν τα μνημονεύει στο σχέδιο της απόφασής της που αποστέλλει στην Επιτροπή.

Στην περίπτωση που, κατά την υποβολή του ΕΕΕΣ, από τον οικονομικό φορέα, δεν συνέτρεχε στο πρόσωπο του κάποιος από τους λόγους αποκλεισμού της παρ. 1 και της παρ. 4, εκτός από την περ. β’ αυτής, του άρθρου 73 του ν. 4412/2016, αλλά η συνδρομή του προέκυψε, κατά τη διάρκεια της παρούσας διαδικασίας (οψιγενής μεταβολή), τα μέτρα αυτοκάθαρσης που επικαλείται, λαμβάνονται υπόψη από την αναθέτουσα αρχή, κατά τη σύνταξη του σχεδίου απόφασής της και εξετάζονται από την Επιτροπή.

Οι διαδικαστικές λεπτομέρειες εξέτασης και επανεξέτασης των επανορθωτικών μέτρων ρυθμίζονται αναλυτικά στην ως άνω υπουργική απόφαση.

2.3.8. Οικονομικός φορέας, σε βάρος του οποίου έχει επιβληθεί η κύρωση του οριζόντιου αποκλεισμού σύμφωνα με τις κείμενες διατάξεις και για το χρονικό διάστημα που αυτή ορίζει, αποκλείεται από την παρούσα διαδικασία σύναψης της σύμβασης.

2.4 Καταλληλότητα άσκησης επαγγελματικής δραστηριότητας

Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας σύμβασης απαιτείται να ασκούν δραστηριότητα συναφή με το αντικείμενο της σύμβασης.

Οι οικονομικοί φορείς που είναι εγκατεστημένοι σε κράτος μέλος της Ευρωπαϊκής Ένωσης απαιτείται να είναι εγγεγραμμένοι σε ένα από τα επαγγελματικά μητρώα ή εμπορικά μητρώα που τηρούνται στο κράτος εγκατάστασής τους ή να ικανοποιούν οποιαδήποτε άλλη απαίτηση ορίζεται στο Παράρτημα XI του Προσαρτήματος Α΄ του ν. 4412/2016. Εφόσον οι οικονομικοί φορείς απαιτείται να διαθέτουν ειδική έγκριση ή να είναι μέλη συγκεκριμένου οργανισμού για να μπορούν να παράσχουν τη σχετική υπηρεσία στη χώρα καταγωγής τους, η αναθέτουσα αρχή μπορεί να τους ζητεί να αποδείξουν ότι διαθέτουν την έγκριση αυτή ή ότι είναι μέλη του εν λόγω οργανισμού ή να τους καλέσει να προβούν σε ένορκη δήλωση ενώπιον συμβολαιογράφου σχετικά με την άσκηση του συγκεκριμένου επαγγέλματος.

Στην περίπτωση οικονομικών φορέων εγκατεστημένων σε κράτος μέλους του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ) ή σε τρίτες χώρες που προσχωρήσει στη ΣΔΣ, ή σε τρίτες χώρες που δεν εμπίπτουν στην προηγούμενη περίπτωση και έχουν συνάψει διμερείς ή πολυμερείς συμφωνίες με την Ένωση σε θέματα διαδικασιών ανάθεσης δημοσίων συμβάσεων, απαιτείται να είναι εγγεγραμμένοι σε αντίστοιχα επαγγελματικά μητρώα.

Οι εγκατεστημένοι στην Ελλάδα οικονομικοί φορείς θα πρέπει να είναι εγγεγραμμένοι στο οικείο επαγγελματικό μητρώο, εφόσον, κατά την κείμενη νομοθεσία, απαιτείται η εγγραφή τους για την υπό ανάθεση υπηρεσία.

Στην περίπτωση ένωσης οικονομικών φορέων, η καταλληλότητα άσκησης επαγγελματικής δραστηριότητας θα πρέπει να καλύπτεται από όλα τα μέλη της ένωσης.

2.5 Οικονομική και χρηματοοικονομική επάρκεια

Όσον αφορά την οικονομική και χρηματοοικονομική επάρκεια για την παρούσα διαδικασία σύναψης σύμβασης, οι οικονομικοί φορείς απαιτείται:

- Να διαθέτουν γενικό ετήσιο κύκλο εργασιών για κάθε μία από τις τρεις (3) τελευταίες διαχειριστικές χρήσεων (2023, 2024, 2025), ίσο με το διπλάσιο του προϋπολογισμού του υπό ανάθεση Έργου. Σε περίπτωση που ο υποψήφιος Ανάδοχος δραστηριοποιείται για χρονικό διάστημα μικρότερο των τριών διαχειριστικών χρήσεων, τότε ο γενικός ετήσιος κύκλος εργασιών για κάθε μία από τις διαχειριστικές χρήσεις που δραστηριοποιείται, θα πρέπει να ισούται με το διπλάσιο του προϋπολογισμού του Έργου. Συμπληρώνεται η οικεία παράγραφος του ΕΕΕΣ.

Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις καλύπτονται αθροιστικά από τα μέλη της ένωσης.

2.6 Τεχνική και επαγγελματική ικανότητα

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για την παρούσα διαδικασία σύναψης σύμβασης, οι οικονομικοί φορείς απαιτείται κατά την διάρκεια των τριών (3) τελευταίων ετών συν το τρέχον του διαγωνισμού, να έχουν εκτελέσει:

1. Ένα (1) έργο προμήθειας, εγκατάστασης και τεχνικής υποστήριξης εξοπλισμού και λογισμικού κυβερνοασφάλειας με υπηρεσίες ασφάλειας δικτύου, ηλεκτρονικού ταχυδρομείου, εσωτερικού δικτύου και MDR για 300 χρήστες.

2. Ένα (1) έργο κεντρικού πληροφοριακού συστήματος υποδομών που να αφορά σε προμήθεια εξυπηρετητών, συστημάτων ασφαλείας και υπηρεσιών μεταφοράς δεδομένων.

3. Δύο (2) έργα τα οποία να περιλαμβάνουν λογισμικό προστασίας με Ελληνικό περιβάλλον λειτουργίας με κεντρική διαχείριση, για τουλάχιστον 1.500 τερματικά (endpoint protection), έκαστο έργο.

4. Τουλάχιστον οκτώ (8) έργα/ενεργούς πελάτες υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών ασφαλείας εγκαταστάσεων πληροφοριακών συστημάτων μέσω Επιχειρησιακού Κέντρου Ασφάλειας (Security Operation Center - SOC), τα οποία να αφορούν τουλάχιστον τρεις (3) διαφορετικούς τομείς. Ο υποψήφιος ανάδοχος οφείλει να υποβάλει σχετική δήλωση με κατάλογο έργων ή/και συμβάσεων. Τουλάχιστον δύο (2) έργα υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών ασφαλείας εγκαταστάσεων πληροφοριακών συστημάτων μέσω Επιχειρησιακού Κέντρου Ασφάλειας (Security Operation Center - SOC) σε κρίσιμες υποδομές, με συνολική αθροιστική αξία τουλάχιστον πεντακόσιες χιλιάδες ευρώ

Παράλληλα και σε ότι αφορά τις υπηρεσίες παρακολούθησης και διαχείρισης περιστατικών ασφαλείας εγκαταστάσεων πληροφοριακών συστημάτων μέσω Επιχειρησιακού Κέντρου Ασφάλειας (Security Operation Centre - SOC), ο υποψήφιος ανάδοχος θα πρέπει να διαθέτει ίδιο Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) εντός Ελλάδος, με ελληνόφωνο προσωπικό και να παρέχει σχετικές υπηρεσίες τουλάχιστον για δέκα (10) συναπτά έτη, στηριζόμενος σε ίδιο κέντρο δεδομένων. Τέλος, θα πρέπει να διαθέτουν και εφαρμόζουν ειδικό πλαίσιο εσωτερικού ελέγχου κυβερνοασφάλειας SOC2 Type II.

Επίσης, ο κατασκευαστής της πλατφόρμας SIEM (Security Information Event Management) θα πρέπει να διαθέτει φυσική παρουσία και εγκαταστάσεις εντός Ελλάδος.

5. Τρία (3) έργα συμβουλευτικών υπηρεσιών συμμόρφωσης σε δημόσιους οργανισμούς.

6. Ένα (1) έργο υπηρεσιών διείσδυσης και ελέγχου ευπαθειών δικτύων και πληροφοριακού περιβάλλοντος σε δημόσιο οργανισμό ή κρίσιμη υποδομή.

Ο συνολικός προϋπολογισμός των ανωτέρω έργων θα πρέπει να είναι διπλάσιος του προϋπολογισμού της διακήρυξης.

Ως ημερομηνία ολοκλήρωσης έργου, θεωρείται η ημερομηνία του πρωτόκολλου οριστικής παραλαβής ή της βεβαίωσης εκτέλεσης έργου.

2.7 Πρότυπα διασφάλισης ποιότητας

Οι οικονομικοί φορείς για την παρούσα διαδικασία σύναψης σύμβασης οφείλουν να συμμορφώνονται με:

- το πρότυπο ISO 9001:2015
- το πρότυπο ISO 14001:2015
- το πρότυπο ISO 27001:2013
- το πρότυπο ISO 20000-1:2018
- το πρότυπο ISO 22301:2019
- το πρότυπο ISO 37001:2016
- το πρότυπο ISO 45001:2018
- το πρότυπο ISO 50001:2018

ή ισοδύναμα, με πεδία εφαρμογής:

- Ανάπτυξη εφαρμογών επιχειρησιακής λειτουργίας – συνέχειας
- Συμβουλευτικές υπηρεσίες ασφάλειας διαδικτύου (Cyber Security)
- Παροχή Υπηρεσιών Ασφαλούς Διαγραφής και Καταστροφής Ψηφιακών Δεδομένων

Η αναθέτουσα αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, εδρεύοντες και σε άλλα κράτη - μέλη. Επίσης, κάνει δεκτά άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο ενδιαφερόμενος οικονομικός φορέας δεν είχε τη δυνατότητα να αποκτήσει τα εν λόγω πιστοποιητικά εντός των σχετικών προθεσμιών για λόγους για τους οποίους δεν ευθύνεται ο ίδιος, υπό την προϋπόθεση ότι ο οικονομικός φορέας αποδεικνύει ότι τα προτεινόμενα μέτρα διασφάλισης ποιότητας πληρούν τα απαιτούμενα πρότυπα διασφάλισης ποιότητας.

Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις πρέπει να καλύπτονται αθροιστικά από τα μέλη της ένωσης.

2.8 Στήριξη στην ικανότητα τρίτων – Υπεργολαβία

2.8.1. Στήριξη στην ικανότητα τρίτων

Οι οικονομικοί φορείς μπορούν, όσον αφορά τα κριτήρια της οικονομικής και χρηματοοικονομικής επάρκειας και τα σχετικά με την τεχνική και επαγγελματική ικανότητα, να στηρίζονται στις ικανότητες άλλων φορέων, ασχέτως της νομικής φύσης των δεσμών τους με αυτούς. Στην περίπτωση αυτή, αποδεικνύουν ότι θα έχουν στη διάθεσή τους τους αναγκαίους πόρους, με την προσκόμιση της σχετικής δέσμευσης των φορέων στην ικανότητα των οποίων στηρίζονται.

Ειδικά, όσον αφορά στα κριτήρια επαγγελματικής ικανότητας που σχετίζονται με τους τίτλους σπουδών και τα επαγγελματικά προσόντα που ορίζονται στην περίπτωση στ΄ του Μέρους ΙΙ του Παραρτήματος XII του Προσαρτήματος Α΄ του ν. 4412/2016 ή με την σχετική επαγγελματική εμπειρία, οι οικονομικοί φορείς, μπορούν να στηρίζονται στις ικανότητες άλλων φορέων, μόνο, εάν οι τελευταίοι θα εκτελέσουν τις εργασίες ή τις υπηρεσίες για τις οποίες απαιτούνται οι συγκεκριμένες ικανότητες.

Όταν οι οικονομικοί φορείς στηρίζονται στις ικανότητες άλλων φορέων όσον αφορά τα κριτήρια που σχετίζονται με την απαιτούμενη με τη διακήρυξη οικονομική και χρηματοοικονομική επάρκεια, οι εν λόγω οικονομικοί φορείς και αυτοί στους οποίους στηρίζονται είναι από κοινού υπεύθυνοι για την εκτέλεση της σύμβασης.

Υπό τους ίδιους όρους οι ενώσεις οικονομικών φορέων μπορούν να στηρίζονται στις ικανότητες των συμμετεχόντων στην ένωση ή άλλων φορέων.

Η αναθέτουσα αρχή ελέγχει αν οι φορείς, στις ικανότητες των οποίων προτίθεται να στηριχθεί ο οικονομικός φορέας, πληρούν κατά περίπτωση τα σχετικά κριτήρια επιλογής και εάν συντρέχουν λόγοι αποκλεισμού. Ο οικονομικός φορέας υποχρεούται να αντικαταστήσει έναν φορέα στην ικανότητα του οποίου στηρίζεται, εφόσον ο τελευταίος δεν πληροί το σχετικό κριτήριο επιλογής ή για τον οποίο συντρέχουν λόγοι αποκλεισμού, εντός προθεσμίας τριάντα (30) ημερών από την σχετική ηλεκτρονική πρόσκληση από την σχετική πρόσκληση της αναθέτουσας αρχής, η οποία απευθύνεται στον οικονομικό φορέα μέσω της λειτουργικότητας «Επικοινωνία» του ΕΣΗΔΗΣ. Ο φορέας που αντικαθιστά φορέα του προηγούμενου εδαφίου δεν επιτρέπεται να αντικατασταθεί εκ νέου.

2.8.2. Υπεργολαβία

Ο οικονομικός φορέας αναφέρει στην προσφορά του το τμήμα της σύμβασης που προτίθεται να αναθέσει υπό μορφή υπεργολαβίας σε τρίτους, καθώς και τους υπεργολάβους που προτείνει. Στην περίπτωση που ο προσφέρων αναφέρει στην προσφορά του ότι προτίθεται να αναθέσει τμήμα(τα) της σύμβασης υπό μορφή υπεργολαβίας σε τρίτους σε ποσοστό που υπερβαίνει το τριάντα τοις εκατό (30%) της συνολικής αξίας της σύμβασης, η αναθέτουσα αρχή ελέγχει ότι δεν συντρέχουν οι λόγοι αποκλεισμού. Ο οικονομικός φορέας υποχρεούται να αντικαταστήσει έναν υπεργολάβο, εφόσον συντρέχουν στο πρόσωπό του λόγοι αποκλεισμού.

3. Κριτήρια Ανάθεσης

3.1 Κριτήριο ανάθεσης

Κριτήριο ανάθεσης της Σύμβασης είναι **η πλέον συμφέρουσα από οικονομική άποψη προσφορά βάσει βέλτιστης σχέσης ποιότητας – τιμής,** η οποία εκτιμάται βάσει των κάτωθι κριτηρίων:

ΚΡΙΤΗΡΙΟ	ΠΕΡΙΓΡΑΦΗ	ΣΥΝΤΕΛΕΣΤΗΣ ΒΑΡΥΤΗΤΑΣ
Κ1	**Βαθμολογία Χαρακτηριστικών Προσφερόμενου Εξοπλισμού και Λογισμικού** Η κάλυψη των τεχνικών προδιαγραφών του προσφερόμενου εξοπλισμού, δηλαδή των πινάκων 1 έως 9 του Μέρους Α «Εξοπλισμός – Λογισμικά» του Παραρτήματος ΙΙ «Τεχνική Προσφορά» της παρούσας. Θα αξιολογηθούν ανώτερα τεχνικά χαρακτηριστικά ή πρόσθετες δυνατότητες, σε σχέση με τις ελάχιστες απαιτήσεις της Διακήρυξης.	**20%**
Κ2	**Βαθμολογία Ποιότητας Υπηρεσιών και Λειτουργίας του Security Operation Center** Θα αξιολογηθούν η παροχή βελτιωμένων υπηρεσιών σε σχέση με τις ελάχιστες απαιτούμενες από τον Πίνακα Β1 του του Παραρτήματος ΙΙ «Τεχνική Προσφορά» της παρούσας και η παροχή πρόσθετων λειτουργιών από το Security Operation Center, σε σχέση με τις ελάχιστες απαιτήσεις	**30%**

	του Πίνακα Β1 του του Παραρτήματος ΙΙ «Τεχνική Προσφορά» της παρούσας.	
Κ3	**Βαθμολογία Υπηρεσιών Εκπαίδευσης** Θα αξιολογηθούν οι υπηρεσίες εκπαίδευσης του προσωπικού της αναθέτουσας Αρχής, σύμφωνα με το «Πλάνο Εκπαίδευσης» το οποίο περιγράφεται στο άρθρο Α3.2.5 Υπηρεσίες Εκπαίδευσης του Παραρτήματος Ι «Αναλυτική Περιγραφή Φυσικού και Οικονομικού Αντικειμένου της Σύμβασης» της παρούσας.	**5%**
Κ4	**Κατανόηση Περιβάλλοντος και Ειδικών Απαιτήσεων Έργου** Αξιολογούνται: • Συνολική κατανόηση του επιχειρησιακού, τεχνολογικού, λειτουργικού και οργανωτικού περιβάλλοντος του Έργου. • Κατανόηση αντικειμένου, ειδικών απαιτήσεων – ιδιαιτεροτήτων, σκοπού και των στόχων του Έργου. • Αναγνώριση κρίσιμων παραγόντων επιτυχίας του Έργου και εντοπισμός ενδεχόμενων προβλημάτων / κινδύνων και προτάσεις αντιμετώπισης αυτών.	**15%**
Κ5	**Μεθοδολογία Υλοποίησης και Διαχείρισης Έργου** Αξιολογείται: • Αρτιότητα και καταλληλότητα της μεθόδου που θα ακολουθήσει ο ανάδοχος για την ανάλυση απαιτήσεων και την υλοποίηση του έργου. • Οργάνωση, διοίκηση επικοινωνία και διαδικασίες υλοποίησης έργου. • Ανάλυση σε φάσεις, χρονοδιάγραμμα, παραδοτέα • Παροχή τυχόν επιπλέον υπηρεσιών, οι οποίες κρίνονται αναγκαίες για την επιτυχή ολοκλήρωση του έργου και οι οποίες δεν έχουν προβλεφθεί στην προκήρυξη	**15%**
Κ6	**Ομάδα Έργου** Αξιολογούνται: • Η σύνθεση και δομή της Ομάδας. • Η εμπειρία και η εξειδίκευση των στελεχών της Ομάδας, σε σχέση με τις ανάγκες του έργου. • Η διαθεσιμότητα και αποκλειστικότητα των στελεχών της Ομάδας. • Η οργανωτική και διαχειριστική ικανότητα, όπως τεκμηριώνεται από την επιτυχή ολοκλήρωση συγκρίσιμων έργων.	**15%**
	ΑΘΡΟΙΣΜΑ ΣΥΝΟΛΟΥ ΣΥΝΤΕΛΕΣΤΩΝ ΒΑΡΥΤΗΤΑΣ	**100%**

3.2 Βαθμολόγηση και κατάταξη προσφορών

Η βαθμολόγηση κάθε κριτηρίου αξιολόγησης κυμαίνεται από 100 βαθμούς στην περίπτωση που ικανοποιούνται ακριβώς όλοι οι όροι των τεχνικών προδιαγραφών, αυξάνεται δε μέχρι τους 150 βαθμούς όταν υπερκαλύπτονται οι απαιτήσεις του συγκεκριμένου κριτηρίου**.**

Κάθε κριτήριο αξιολόγησης βαθμολογείται αυτόνομα με βάση τα στοιχεία της προσφοράς.

Η σταθμισμένη βαθμολογία του κάθε κριτηρίου θα προκύπτει από το γινόμενο του επιμέρους συντελεστή βαρύτητας επί τη βαθμολογία του, η δε συνολική βαθμολογία της προσφοράς θα προκύπτει από το άθροισμα των σταθμισμένων βαθμολογιών όλων των κριτηρίων.

Η συνολική βαθμολογία της τεχνικής προσφοράς υπολογίζεται με βάση τον παρακάτω τύπο:

Τ= σ1 × Κ1 + σ2 × Κ2 +……+ σν × Κν

Όπου:
σν είναι ο συντελεστής βαρύτητας του κάθε κριτηρίου αξιολόγησης και ισχύει σ1+σ2+σ3+…+σν=1 (ή 100%) και
Κν είναι η βαθμολογία που έλαβε η τεχνική προσφορά στην απαίτηση της προδιαγραφής

Κριτήρια με βαθμολογία μικρότερη από 100 βαθμούς (ήτοι που δεν καλύπτουν/παρουσιάζουν αποκλίσεις από τις τεχνικές προδιαγραφές της παρούσας) επιφέρουν την **απόρριψη της προσφοράς**.

Ο τελικός βαθμός της προσφοράς του οικονομικού φορέα (προσφέροντος) προκύπτει από τον τύπο:

Β = 0,80 x (Τ/Tmax) + 0,2 x (Omin/Ο)

όπου:

Β = Συνολική βαθμολογία της προσφοράς

Τ = Συνολική βαθμολογία τεχνικής προσφοράς,

Tmax = Συνολική βαθμολογία της καλύτερης τεχνικής προσφοράς κατά την τεχνική αξιολόγηση (μεταξύ των αποδεκτών προσφορών)

Omin = Τιμή χαμηλότερης οικονομικής προσφοράς κατά την οικονομική αξιολόγηση (μεταξύ των αποδεκτών προσφορών)

Ο = Τιμή οικονομικής προσφοράς,

Οι βαθμολογίες στρογγυλοποιούνται στο δεύτερο δεκαδικό ψηφίο. Το σύνολο των αποδεκτών προσφορών καταγράφονται σε Συγκριτικό Πίνακα, κατά φθίνουσα σειρά του τελικού βαθμού (Β). Σε περίπτωση ισοβαθμίας, οι προσφορές που ισοβαθμούν κατατάσσονται κατά φθίνουσα σειρά του βαθμού τεχνικής αξιολόγησης (Τ).

Η πρώτη στον Συγκριτικό Πίνακα κατάταξης (δηλαδή αυτή με την υψηλότερη συνολική βαθμολογία), θεωρείται η πλέον συμφέρουσα προσφορά.

ΜΕΡΟΣ Α - ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ

Α1 Περιβάλλον του Έργου

Α1.1 Συνοπτική Περιγραφή των υπηρεσιών και της λειτουργίας της Α.Α.

Η Αναθέτουσα Αρχή είναι η Μονάδα Οργάνωσης της Διαχείρισης Αναπτυξιακών Προγραμμάτων (Μ.Ο.Δ.) Α.Ε., η οποία τελεί υπό την εποπτεία του Υπουργού Εθνικής Οικονομίας και Οικονομικών και ανήκει στους φορείς της Γενικής Κυβέρνησης (υποτομέας Κεντρικής Κυβέρνησης).

Η ΜΟΔ Α.Ε. ιδρύθηκε το 1996 με τον ν.2372/1996, ο οποίος στη συνέχεια συμπληρώθηκε και τροποποιήθηκε με τους ν.2860/2000 (άρθρο 18), ν.2937/2001 (άρθρο 37), ν.3193/2003 (άρθρο 17) και ν.3336/2005 (άρθρο 7), καθώς και την Υπουργική Απόφαση 25045/314 Γ ΚΠΣ.

Με το άρθρο 33 του ν.3614/2007 (Α΄ 267), όπως έκτοτε τροποποιήθηκε και ισχύει, κωδικοποιήθηκε το καταστατικό της ΜΟΔ Α.Ε. σε ενιαίο κείμενο (αρ. ΓΕΜΗ: 122135901000).

Σύμφωνα με το καταστατικό της, η ΜΟΔ Α.Ε. υπάγεται στον παραπάνω ν.3614/2007, άρθρο 33 και συμπληρωματικά στις διατάξεις του Κ.Ν. 2190/1920 (αναθεωρηθέντος πλήρως με τον ν.4548/2018 περί αναμόρφωσης του δικαίου των ΑΕ) και στις διατάξεις του άρθρου 36 του ν.849/1978 (Α΄ 232), όπως κάθε φορά ισχύουν.

Η ΜΟΔ Α.Ε. είναι ανώνυμη εταιρία μη κερδοσκοπικού χαρακτήρα με μοναδικό μέτοχο το Ελληνικό Δημόσιο. Η Εταιρία λειτουργεί χάριν του δημοσίου συμφέροντος κατά τους κανόνες της ιδιωτικής οικονομίας και εποπτεύεται από τον Υπουργό Εθνικής Οικονομίας και Οικονομικών.

Σκοπός της Εταιρίας είναι κυρίως η επιστημονική και τεχνική υποστήριξη της διαχείρισης και εφαρμογής προγραμμάτων που συγχρηματοδοτούνται από την Ευρωπαϊκή Ένωση, από τον Ευρωπαϊκό Οικονομικό Χώρο (Ε.Ο.Χ.) ή/και από εθνικούς πόρους, η οργάνωση και η κάλυψη των αναγκών σε εξειδικευμένο ανθρώπινο δυναμικό και σε μεταφορά τεχνογνωσίας για τη βελτίωση της διοικητικής δομής καθώς και η κάλυψη αναγκών στέγασης και υλικοτεχνικής υποδομής των εμπλεκόμενων με το σχεδιασμό, διαχείριση, παρακολούθηση και έλεγχο των αναπτυξιακών προγραμμάτων.

Η έδρα της Εταιρίας είναι στο Δήμο Αθηναίων και τα γραφεία της βρίσκονται επί της οδού Λουΐζης Ριανκούρ αρ. 78Α.

Η Εταιρία έχει εγκαταστήσει και εφαρμόζει Σύστημα Διαχείρισης Ποιότητας κατά το πρότυπο ISO 9001:2015 για «Υποστήριξη της διαχείρισης και εφαρμογής του ΕΣΠΑ και άλλων αναπτυξιακών προγραμμάτων». Επιπλέον, διαθέτει επάρκεια υλοποίησης έργων ΕΣΠΑ και βεβαίωση διαχειριστικής επάρκειας για την υλοποίηση συγχρηματοδοτούμενων έργων.

Α1.2 Οργανωτική δομή της Α.Α.

Η ΜΟΔ διοικείται από 9μελές Διοικητικό Συμβούλιο τριετούς θητείας.

Η Κεντρική Υπηρεσία της ΜΟΔ εδρεύει στην Αθήνα και αποτελείται από τις παρακάτω υπηρεσίες:

- Γενικός Διευθυντής
- Γραμματεία Διοίκησης
- Υπηρεσία Νομικής Υποστήριξης
- Μονάδα Εσωτερικού Ελέγχου

  - Τμήμα Μεθοδολογίας, Σχεδιασμού Εσωτερικών Ελέγχων & Συμβουλευτικών Υπηρεσιών
  - Τμήμα Διενέργειας Εσωτερικών Ελέγχων
- Υπεύθυνος Ασφάλειας Προσωπικών Δεδομένων (DPO)
- Υπεύθυνος Ποιότητας
- Τμήμα Υποστήριξης Προγραμματισμού & Επικοινωνίας (ΤΥΠΕ)
- Διεύθυνση Διαχειριστικών & Υποστηρικτικών Υπηρεσιών
  - Ομάδα Υποστήριξης Δικαιούχων σε Νησιωτικές & Απομακρυσμένες Περιοχές
  - Ομάδα Υποστήριξης Δικαιούχων σε Ορεινές και Μειονεκτικές περιοχές
  - Ομάδα Υποστήριξης Δράσεων για Ευπαθείς Ομάδες Πληθυσμού και Δικαιούχων του Ευρωπαϊκού Κοινωνικού Ταμείου
  - Ομάδα Τεχνικής Υποστήριξης Περιβάλλοντος
  - Ομάδα Υποστήριξης Παρεμβάσεων Κρατικών Ενισχύσεων
- Διεύθυνση Εφαρμογών Πληροφορικής και Ψηφιακής Τεχνολογίας
  - Τμήμα Υποστήριξης Ηλεκτρονικών Υποδομών και Δικτύων
  - Τμήμα Διαχείρισης και Υποστήριξης Πληροφοριακού Κέντρου και Υπολογιστικού Νέφους (Cloud)
  - Τμήμα Υποστήριξης Εφαρμογών Διαδικτύου
  - Τμήμα Ανάπτυξης και Υποστήριξης του Πληροφοριακού Συστήματος Κρατικών Ενισχύσεων (ΠΣΚΕ)
  - Ομάδα Υποστήριξης Εφαρμογών Πληροφορικής του Ολοκληρωμένου Πληροφοριακού Συστήματος (ΟΠΣ)
- Διεύθυνση Οικονομικών και Διοικητικών Υπηρεσιών
  - Τμήμα Οικονομικής Διαχείρισης
  - Τμήμα Διοικητικής Διαχείρισης
  - Τμήμα Διαχείρισης Τεχνικής Βοήθειας
- Διεύθυνση Προμηθειών
  - Τμήμα Προμηθειών και Υπηρεσιών
  - Τμήμα Ανάπτυξης Κτιριακών Υποδομών και Υλικοτεχνικής Υποδομής
- Διεύθυνση Τεχνικής Υπηρεσίας (ΔΤΥ)
  - Τμήμα Μελετών Τεχνικών Έργων
  - Τμήμα Μελετών Ειδικών Έργων
  - Τμήμα Εκτέλεσης Τεχνικών Έργων
- Διεύθυνση Υπηρεσιών Διοίκησης και Ανάπτυξης Ανθρώπινου Δυναμικού
  - Τμήμα Υπηρεσιών Στελέχωσης και Διοίκησης Ανθρώπινου Δυναμικού
  - Τμήμα Εκπαίδευσης και Ανάπτυξης Ανθρώπινου Δυναμικού
- Διεύθυνση Υπηρεσιών Σχεδιασμού και Οργάνωσης

- Τμήμα Μελετών

Η Διεύθυνση Εφαρμογών Πληροφορικής και Ψηφιακής Τεχνολογίας είναι αρμόδια για τον σχεδιασμό και την ανάπτυξη εφαρμογών πληροφορικής και ψηφιακής τεχνολογίας καθώς και για την εγκατάσταση και την λειτουργία των πληροφοριακών συστημάτων στους φορείς Διαχείρισης Προγραμμάτων και Υλοποίησης των Έργων:

- Προμηθεύει, εγκαθιστά και υποστηρίζει τις υποδομές Πληροφορικής και Τηλεπικοινωνιών των Ειδικών Υπηρεσιών (ΕΥ)
- Λειτουργεί το Δίκτυο Πληροφοριών (INTRANET) του ΚΠΣ / ΕΣΠΑ
- Εξασφαλίζει την καλή λειτουργία, ασφάλεια και συντήρηση των εγκατεστημένων συστημάτων πληροφορικής στις ΕΥ
- Υλοποιεί, υποστηρίζει και φιλοξενεί ιστοχώρους των ΕΥ
- Σχεδιάζει και αναπτύσσει συστήματα ηλεκτρονικής διαχείρισης
- Μεταφέρει τεχνογνωσία στο τεχνικό και υποστηρικτικό προσωπικό των ΕΥ σχετικά με νέα εργαλεία και πληροφοριακά συστήματα
- Υποστηρίζει όλους τους εμπλεκόμενους με το Ολοκληρωμένο Πληροφοριακό Σύστημα – ΟΠΣ «ΕΡΓΟΡΑΜΑ» φορείς και εξασφαλίζει την καλή λειτουργία του Πληροφοριακού Συστήματος. Υποστηρίζει όλα τα υποσυστήματα του ΟΠΣ, και πιο συγκεκριμένα:
  - ✓ ΕΣΠΑ
  - ✓ Κοινοτικό Πλαίσιο Στήριξης / Κοινοτικές Πρωτοβουλίες
  - ✓ Ταμείο Συνοχής
  - ✓ Πρόγραμμα Δημοσίων Επενδύσεων
  - ✓ Ιδιωτικές Επενδύσεις

Α1.3 Υφιστάμενη κατάσταση

Η Αναθέτουσα Αρχή έχει δημιουργήσει και λειτουργεί στις εγκαταστάσεις της σύγχρονο data center που καλύπτει όλες τις σύγχρονες προδιαγραφές λειτουργικότητας και ασφάλειας.

Συγκεκριμένα διαθέτει:

- Συστήματα κλιματισμού. Πλήρης αναπληρωματικότητα (redundancy) με οκτώ μονάδες τύπου closed control, τέσσερις εν λειτουργία και τέσσερις αναπληρωματικές σε αναμονή (stand by) με αυτόματη εναλλαγή.
- Τροφοδοσία ηλεκτρικού ρεύματος. Πλήρης αναπληρωματικότητα (redundancy) με UPS 120 KVA και γεννήτρια Diesel ισχύος 360 KVA.
- Αυτόματο σύστημα πυρόσβεσης με αδρανές αέριο που δεν προκαλεί βλάβες στον εξοπλισμό.
- Σύστημα ελεγχόμενης πρόσβασης με καταγραφικό.
- Ισχυρό σύστημα προστασίας έναντι εισβολών από το Διαδίκτυο.
- Διπλή σύνδεση με παρόχους. Σύνδεση οπτικής ίνας με ΟΤΕ και σύνδεση με το «Σύζευξις».
- Μεγάλες δυνατότητες επέκτασης για φιλοξενία νέων κεντρικών υποδομών.

Είναι ήδη διακηρυγμένη ως πολιτική και τεχνολογική επιλογή η συγκέντρωση υποδομών και διαμοιρασμού του λογισμικού σε αποκεντρωμένα σημεία (Virtual Servers, Cloud Computing). Η φιλοσοφία της τεχνικής, είναι αντί να υπάρχει υποδομή (servers) σε μεμονωμένα αποκεντρωμένα σημεία χωρίς επαρκή υπολογιστική ισχύ, ασφάλεια και υποστήριξη, αυτή να συγκεντρώνεται σε λίγα κεντρικά οργανωμένα data centers και να μοιράζεται μέσω δικτύου στους χρήστες, οι οποίοι διατηρούν την αίσθηση και τις δυνατότητες που θα είχαν εάν η υποδομή ήταν δίπλα τους.

Η ΜΟΔ διαβλέποντας τα προφανή οφέλη της τεχνολογίας αυτής (οικονομίες κλίμακας σε υποδομή και προσωπικό, ασφάλεια, λειτουργικότητα κ.λ.π.), σχεδίασε, υλοποίησε και έχει ήδη σε λειτουργία επτά φάρμες με φυσικούς servers, στους οποίους λειτουργεί σημαντικός αριθμός από εικονικούς (virtual) servers. Παράλληλα διαθέτει virtual servers σε συνεργαζόμενους φορείς για να εγκαταστήσουν εφαρμογές τους, εκμεταλλευόμενες την υποδομή, ασφάλεια και λειτουργικότητα του Data Center, οι οποίες δεν είναι δυνατόν να υπάρχουν σε μεμονωμένα σημεία.

Το μεγαλύτερο μέρος του εξοπλισμού του Data Center της Αναθέτουσας Αρχής αποτελείται από εξοπλισμό του οποίου η προμήθεια έγινε στο παρελθόν μέσω Ανοικτού Διεθνούς Διαγωνισμού.

Συγκεκριμένα αποτελείται από 46 Dell PowerEdge M630 Blade Servers και 10 Dell PowerEdge M820 Blade Servers. Οι εξυπηρετητές αυτοί συνδέονται μέσω δύο Dell Brocade 6520 SAN Switches σε εξωτερικό σύστημα δίσκων (SAN) Dell Compellent SC8000 Storage Center, συνολικής ωφέλιμης χωρητικότητας >150TB.

Παράλληλα χρησιμοποιείται σύστημα λήψης αντιγράφων ασφαλείας σε ταινία (B2T) Dell ML6010 LTO-6 Tape Library και σύστημα αποθήκευσης εφεδρικών αντιγράφων σε δίσκο (B2D), αποτελούμενο από το σύστημα αποθήκευσης Dell PowerVault ME4012, με συνολική ωφέλιμη χωρητικότητα >80TB

Στο Data Center της Αναθέτουσας Αρχής φιλοξενείται μεγάλος αριθμός ιστοτόπων (web sites) και ευρύτερα διαδικτυακών εφαρμογών, οι οποίες έχουν αναπτυχθεί είτε εσωτερικά (από τη Διεύθυνση Εφαρμογών Πληροφορικής & Ψηφιακής Τεχνολογίας), είτε από αναδόχους, και τους διαχειρίζεται ομάδα στελεχών της Διεύθυνσης Εφαρμογών Πληροφορικής & Ψηφιακής Τεχνολογίας. Διατίθεται επίσης σημαντικός αριθμός υπολογιστικών συστημάτων τα οποία εξυπηρετούν τις ανάγκες τόσο της Κεντρικής Υπηρεσίας της Αναθέτουσας Αρχής, όσο και των υποστηριζόμενων από αυτή Φορέων (Ειδικών Υπηρεσιών Διαχείρισης και λοιπών εμπλεκόμενων υπηρεσιών στην διαχείριση και έλεγχο του ΕΣΠΑ).

Οι ανάγκες αυτές αφορούν αφενός βασικές υποδομές (Active Directory, Mail, Proxy Server κλπ) και αφετέρου Πληροφοριακά Συστήματα για εσωτερική αλλά και δημόσια χρήση.

Το δίκτυο δεδομένων της Αναθέτουσας Αρχής αποτελείται από 30 και πλέον, απομακρυσμένα σημεία (remote sites, που αποτελούν τα ανεξάρτητα υπο-δίκτυα των Ειδικών Υπηρεσιών του ΕΣΠΑ) .

Ο υφιστάμενος αριθμός δικτυακού εξοπλισμού στο σύνολο του δικτύου που υποστηρίζει η ΜΟΔ:

- Routers ≈ 30
- Firewalls ≈ 20

Ο κατασκευαστής των παραπάνω συσκευών είναι η εταιρία CISCO.

Στην Κεντρική Υπηρεσία της Αναθέτουσας Αρχής βρίσκονται ≈ 220 workstation και laptops ενώ στα απομακρυσμένα σημεία βρίσκονται ≈ 1400 workstations

Τα απομακρυσμένα σημεία συνδέονται με το Internet είτε μέσω MPLS VPN δικτύου με την Κεντρική Υπηρεσία είτε μέσω ανεξάρτητης σύνδεσης ΣΥΖΕΥΞΙΣ Ι και ΣΥΖΕΥΞΙΣ ΙΙ. Η σύνδεση MPLS VPN γίνεται με χρήση είτε ADSL είτε VDSL τεχνολογίας.

<u>Στο data center της ΜΟΔ υπάρχουν 3 ανεξάρτητες συνδέσεις Internet:</u>

- Απευθείας σύνδεση με OTE metro Ethernet με ταχύτητα 1000mbps

- Σύνδεση metro Ethernet με το ΣΥΖΕΥΞΙΣ ταχύτητας 300mbps
- VDSL σύνδεση 30mbps για τις εφαρμογές τηλεδιάσκεψης και την παροχή ανεξάρτητου ασύρματου δικτύου WiFi.

Στο datacenter της Αναθέτουσας Αρχής υπάρχει σύγχρονος εξοπλισμός Next generation firewall **Fortigate 601E** σε τοπολογία active-passive με ενεργή υποστήριξη από την κατασκευάστρια εταιρία έως **23/4/2026**. Το σύστημα firewalling Fortigate 601E συνοδεύεται από άδειες IPS, Antivirus και Web filtering με διάρκεια ισχύος έως 23/4/2026. Παράλληλα η ΜΟΔ έχει προμηθευτεί και χρησιμοποιεί :

- 1 Fortinet FortiMAIL virtual appliance για την προστασία του συστήματος ηλεκτρονικής αλληλογραφίας με ενεργή υποστήριξη ανανέωσης των ορισμών antivirus και antispam έως **29/3/2029**
- Fortinet FortiAnalyzer που χρησιμοποιείται για τοπικό logging & reporting των χρησιμοποιούμενων συσκευών.
- 1600 άδειες χρήσης Microsoft E5 security με διάρκεια ισχύς έως 31/12/2026. Οι άδειες Microsoft E5 security περιλαμβάνουν τα κάτωθι features:
  - Microsoft Entra ID P2
  - Microsoft Defender XDR
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Identity

Τονίζεται ότι η ΜΟΔ Α.Ε χρησιμοποιεί τις υπηρεσίες Microsoft Azure, ακολουθώντας φιλοσοφία hybrid cloud. Πιο συγκεκριμένα σημαντικό μέρος των γραμματοκιβωτίων των χρηστών έχει μεταφερθεί στις Υπηρεσίες Microsoft / Office 365 χρησιμοποιώντας παράλληλα λύσεις αποθήκευσης και διαμοιρασμού αρχείων όπως Microsoft OneDrive, Sharepoint online και λύσεις collaboration Microsoft Teams.

Επίσης το Microsoft Azure περιβάλλον χρησιμοποιείται για την εφεδρική αποθήκευση αντιγράφων ασφαλείας με τις εφαρμογές Microsoft Azure Backup Server και DPM Backup to Azure, ενώ έχει υλοποιηθεί και περιβάλλον Disaster Recovery ειδικά για το Πληροφοριακό Σύστημα Κρατικών Ενισχύσεων χρησιμοποιώντας την τεχνολογία Azure ASR (Site Recovery) μέσω Azure Site to Site VPN.

Τέλος οι εφαρμογές ασφάλειας δεδομένων και πληροφοριακών συστημάτων που χρησιμοποιούνται στο Azure είναι οι:

- Azure Arc
- Azure Sentinel
- Azure Security Center
- Azure LogAnalytics

Α2 Σκοπός και στόχοι της Σύμβασης

Α2.1 Περιγραφή των αναγκών της Αναθέτουσας Αρχής – Σκοπιμότητα και Αναμενόμενα Οφέλη

Σκοπός της παρούσας διακήρυξης αποτελεί η προμήθεια εξοπλισμού, λογισμικού και η παροχή υπηρεσιών ενίσχυσης της ασφάλειας του δικτύου δεδομένων της ΜΟΔ Α.Ε.

Βασική προϋπόθεση υλοποίησης του έργου, αποτελεί η εκμετάλλευση από τον ανάδοχο στο έπακρο του εξοπλισμού και των λογισμικών που ήδη διαθέτει η Αναθέτουσα Αρχή.

Οι προτάσεις για προμήθεια νέου εξοπλισμού και λογισμικού θα πρέπει να γίνουν με γνώμονα την πλήρη ομοιογένεια των υφιστάμενων και νέων συστημάτων, ώστε να αποφευχθεί οποιαδήποτε μελλοντική ασυμβατότητα, και να καλυφθούν όλα τα πιθανά κενά της ασφάλειας δικτύου, αποφεύγοντας παράλληλα την αύξηση της πολυπλοκότητας στην χρήση και τη διαχείριση των δικτυακών υποδομών και των υποδομών ασφαλείας.

Μέσω του παρόντος έργου η Αναθέτουσα Αρχή επιδιώκει:

1. Την υιοθέτηση νέων τεχνολογιών και ρυθμίσεων ασφαλούς αρχιτεκτονικής για την προστασία της δικτυακής υποδομής του Οργανισμού.
2. Υλοποίηση αρχιτεκτονικής που βασίζεται στην αρχή defense in depth, ώστε εφαρμόζονται μέτρα και μηχανισμοί ασφάλειας σε μορφή διαδοχικών στρωμάτων και ζωνών σε όλο το εύρος του δικτύου και των δεδομένων του.
3. Υιοθέτηση της αρχής της ελάχιστης λειτουργικότητας (Least Functionality) ρυθμίζοντας το σύνολο των συστημάτων της ΜΟΔ έτσι ώστε να παρέχουν μόνο τις λειτουργίες και υπηρεσίες που υποστηρίζουν την επιχειρησιακή αποστολή του Οργανισμού.
4. Ενοποίηση όλων των επιμέρους συστημάτων ασφάλειας και λειτουργικών οντοτήτων με σύστημα Διαχείρισης και Ανάλυσης Αρχείων Καταγραφής Περιστατικών Ασφάλειας (SIEM).
5. Δημιουργία παραμετροποιήσιμων (custom) κανόνων συσχέτισης (correlation rules) για το σύστημα Διαχείρισης και Ανάλυσης Αρχείων Καταγραφής Περιστατικών Ασφάλειας (SIEM) με χαμηλά στατιστικά λάθος εντοπισμού (false-positive).
6. Την αποτελεσματική ανίχνευση δικτυακών απειλών και επιθέσεων στα τελικά σημεία πριν και μετά τη υλοποίησή τους, εμποδίζοντας τις παραβιάσεις δεδομένων σε πραγματικό χρόνο.
7. Τη μεγιστοποίηση του βαθμού ασφάλειας των υποδομών του οργανισμού με την υλοποίηση συστήματος Διαχείρισης Προνομιακών Προσβάσεων, και την υιοθέτηση της βασικής αρχής ασφάλειας “Least Privilege” κατά τη διαχείριση και χρήση των προσβάσεων.
8. Υλοποίηση αποτελεσματικότερης διαδικασίας λήψης αντιγράφων ασφαλείας (backup) για την προστασία των συστημάτων και πληροφοριών.
9. Την μέγιστη και αποτελεσματική αξιοποίηση των feature ασφαλείας των αδειών Microsoft 365

Όλα τα παραπάνω έχουν ορισθεί βάσει των όσων προβλέπονται από:

- Την Εθνική Στρατηγική ΚυβερνοΑσφάλειας (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω), μέσω της οποίας αναπτύσσεται ο κεντρικός σχεδιασμός της Ελληνικής Πολιτείας αναφορικά με τον τομέα της ασφάλειας στον κυβερνοχώρο.
- Τον Ν. 4577/2018 (Α΄ 199) — Οδηγία (ΕΕ) 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών.
- Τον Γενικό Κανονισμό Προσωπικών Δεδομένων (ΕΕ) 2016/67.
- Το Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και τα Πρότυπα Διαλειτουργικότητας (“e-gif”) (Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, ΥΑΠ/Φ.40.4/1/989/2012 (Β΄ 1301).
- Τις διατάξεις του Ν. 4727/2020 (Α΄ 184) για το Κυβερνητικό Νέφος.

- Τις διατάξεις του Ν. 4727/2020 (Α΄ 184) για την Ηλεκτρονική Προσβασιμότητα που ενσωματώνει την Οδηγία (ΕΕ) 2016/2102.
- Τις διατάξεις του ν. 5610/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις».
- Τις Υπουργικές Αποφάσεις 1689/2025 «Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας» και 1899/2025 «Καθορισμός προσόντων, καθηκόντων, ασυμβιβάστων και υποχρεώσεων του ΥΑΣΠΕ».

Α2.2 Στοιχεία ωριμότητας της Σύμβασης

Η σύμβαση περιλαμβάνεται στην εγκεκριμένη πράξη με τίτλο «Υποστήριξη της διοικητικής οργάνωσης και λειτουργίας των δομών συντονισμού, διαχείρισης και επιτελικών δομών των Υπουργείων, καθώς και του συστήματος διοίκησης και συντονισμού της εφαρμογής συγχρηματοδοτούμενων δράσεων», η οποία έχει ενταχθεί στο Πρόγραμμα «Τεχνική Βοήθεια και Υποστήριξη Δικαιούχων 2021-2027 (ΤΕΒΟ)» με βάση την απόφαση ένταξης με αρ. πρωτ. 123708/21-12-2023, της ΕΥΔ Προγράμματος ΤΕΒΟ με MIS 6005047. Η πράξη χρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο, Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης και Ταμείο Συνοχής) και από εθνικούς πόρους μέσω του ΠΔΕ και ακολουθεί τους κανόνες των συγχρηματοδοτούμενων από το ΕΣΠΑ έργων.

Η διενέργεια του διαγωνισμού έχει εγκριθεί από το Δ.Σ. της Αναθέτουσας Αρχής με την υπ' αριθ. …… (Θέμα ….ο) απόφασή του της …….

Για τη δέσμευση του ποσού, έχει ληφθεί η σχετική απόφαση της Αναθέτουσας Αρχής με θέμα: "Απόφαση Ανάληψης Υποχρέωσης" (ΑΔΑ ……, ΑΔΑΜ ……..).

Α3.3 Τεκμηρίωση σκοπιμότητας/υποδιαίρεσης ή μη της σύμβασης σε τμήματα

Η σύμβαση αφορά ένα ενιαίο αντικείμενο. Όλα τα υπό προμήθεια είδη αποσκοπούν στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και του δικτύου δεδομένων της ΜΟΔ ΑΕ.

Ταυτοχρόνως, οι Υπηρεσίες, οι οποίες αποτελούν και το μεγαλύτερο τμήμα της σύμβασης, σχετίζονται απολύτως με τον υπό προμήθεια εξοπλισμό και λογισμικό, καθώς αφορούν:

- Την εγκατάσταση και παραμετροποίηση του εξοπλισμού και λογισμικού.
- Τον επανασχεδιασμό της υφιστάμενης αρχιτεκτονικής και των ζωνών ασφαλείας του δικτύου δεδομένων της Αναθέτουσας Αρχής, για την βέλτιστη αξιοποίηση του υπό προμήθεια εξοπλισμού και λογισμικού.
- Την εκπαίδευση του προσωπικού της Αναθέτουσας Αρχής στον υπό προμήθεια εξοπλισμό και λογισμικό.
- Την παρακολούθηση και διαχείρισης της Ασφαλείας του δικτύου δεδομένων 24x7 από το Επιχειρησιακό Κέντρο Ασφάλειας SoC (Security Operation Center).
- Την υποστήριξη της διαχείρισης του εξοπλισμού και λογισμικού ασφαλείας από εξειδικευμένο προσωπικό αποτελούμενο (τουλάχιστον 2 στελέχη).

Καθίσταται εμφανές ότι απαιτείται από την πλευρά του Αναδόχου άριστη γνώση του υπό προμήθεια εξοπλισμού και λογισμικού και αντιμετώπισή του ως ένα ενιαίο αντικείμενο με είδη συνεργαζόμενα μεταξύ τους, η οποία, δεδομένου και του μεγάλου αριθμού και της εξειδικευμένης φύσης των υπό προμήθεια ειδών, εξασφαλίζεται με την αντιμετώπιση του έργου ως μίας ενιαίας σύμβασης, με τον Ανάδοχο να

υλοποιεί τόσο την προμήθεια, όσο και την παραμετροποίηση, παρακολούθηση και διαχείριση του εξοπλισμού και λογισμικού.

Α3 Αναλυτικό Αντικείμενο του Έργου

Α3.1 Περιγραφή εξοπλισμού και λογισμικών

Αντικείμενο της σύμβασης αποτελεί η προμήθεια εξοπλισμού και λογισμικού ενίσχυσης της ασφάλειας του δικτύου δεδομένων της Αναθέτουσας Αρχής, που αναλύεται περαιτέρω σε:

1. **Προμήθεια δύο (2) συσκευών Next Generation Firewall (NGF)**
2. **Προμήθεια Web Application Firewall με την μορφή virtual appliance (WAF)**
3. **Προμήθεια δύο (2) Virtual Appliances για την προστασία των χρηστών κατά την περιήγηση στο διαδίκτυο (Web Proxy)**
4. **Προμήθεια Virtual Appliance για την ενιαία διαχείριση των συσκευών NGF, WAF και Web Proxy**
5. **Προμήθεια λογισμικού δημιουργίας αντιγράφων ασφάλειας και αποκατάστασης καταστροφών για 500 εικονικούς εξυπηρετητές**
6. **Προμήθεια λογισμικού Διαχείρισης Προνομιακών Προσβάσεων (Privileged Access Management – PAM).**
7. **Προμήθεια Λογισμικού Ανάλυσης και Παρακολούθησης Δικτύου**
8. **Προμήθεια Λογισμικού Asset Management**
9. **Πλατφόρμα περιορισμού Ransomware**
10. **Επέκταση χρονικής διάρκειας αδειών χρήσης του υφιστάμενου εξοπλισμού (Fortigate 601E, fortimail, fortianalyzer) της Αναθέτουσας Αρχής, ώστε να συμπίπτουν με τις υπό προμήθεια άδειες χρήσης των προϊόντων που αναφέρονται στα σημεία 1 έως 4.**

Το σύνολο του παραπάνω εξοπλισμού και λογισμικών συνοδεύεται από υπηρεσίες επανασχεδιασμού της υφιστάμενης αρχιτεκτονικής και των ζωνών ασφαλείας του δικτύου δεδομένων, υπηρεσίες εγκατάστασης και εκπαίδευσης, καθώς και:

1. **Υπηρεσίες καθημερινής υποστήριξης, για χρονικό διάστημα τριών (3) ετών, από τουλάχιστον δύο (2) άτομα στην διαχείριση συσκευών και λογισμικών ασφάλειας δικτύου και συστημάτων πληροφορικής.**
2. **Υπηρεσίες Ανίχνευσης και Αποτίμησης Ευπαθειών οι οποίες θα περιλαμβάνουν έλεγχο διείσδυσης στο εξωτερικό και εσωτερικό περιβάλλον των υποδομών.**
3. **Υπηρεσίες Παρακολούθησης και Διαχείρισης της Ασφάλειας του Δικτύου Δεδομένων 24 x 7 για χρονικό διάστημα τριών (3) ετών, από Security Operation Center το οποίο θα είναι εγκατεστημένο εντός Ελλάδος.**
4. **Υπηρεσίες Παραμετροποίησης Εξοπλισμού & Λογισμικού**

Οι αναλυτικές τεχνικές προδιαγραφές του ανωτέρω εξοπλισμού δίνονται στο Παράρτημα ΙΙ – Υπόδειγμα Τεχνικής Προσφοράς (Πίνακες Συμμόρφωσης) της παρούσας.

Α3.2 Περιγραφή υπηρεσιών

Θεμελιώδες στοιχείο του παρόντος έργου αποτελούν οι υπηρεσίες :

Α3.2.1 Εγκατάστασης και Παραμετροποίησης

Το σύνολο του παρεχόμενου εξοπλισμού (physical και virtual appliances) και του λογισμικού συνοδεύονται από υπηρεσίες εγκατάστασης και παραμετροποίησης.

Οι υπηρεσίες εγκατάστασης-παραμετροποίησης που θα συνοδεύουν τις «υπηρεσίες Διαχείρισης της Ασφαλείας του δικτύου δεδομένων 24x7 από Επιχειρησιακό Κέντρο Ασφάλειας SoC (Security Operation Center)» θα προσφερθούν από τον Ανάδοχο σε συνεργασία με την Αναθέτουσα Αρχή και αφορούν την εγκατάσταση και παραμετροποίησή και των κατάλληλων αισθητήρων ώστε να μεταφερθούν τα αρχεία καταγραφής και οι δικτυακές ροές από την υποδομή της Αναθέτουσας Αρχής προς την υποδομή SoC του Αναδόχου.

Επίσης θα πρέπει να είναι σε ετοιμότητα η καταγραφή πλήρους δικτυακής κίνησης από κρίσιμα σημεία της υποδομής της Αναθέτουσας Αρχής. Η πλήρη δικτυακή κίνηση θα χρησιμοποιείται για την περαιτέρω διερεύνηση περιστατικού (εάν απαιτείται) καθώς και για αναζήτηση απειλών (threat hunting).

Σε περίπτωση που κατά την περίοδο εγκατάστασης, εμφανισθούν προβλήματα ή διαπιστωθεί ότι δεν πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, ο Ανάδοχος οφείλει να προβαίνει άμεσα στις απαραίτητες βελτιωτικές παρεμβάσεις και αναπροσαρμογές.

Ο ανάδοχος οφείλει να αναλύσει (parsing) και να ενσωματώσει τις ανωτέρω πληροφορίες στα συστήματά του ώστε αξιοποιηθούν στο έπακρο τα στοιχεία που συλλέγονται.

Ο Ανάδοχος υποχρεούται να οργανώσει και να συμμετέχει σε δοκιμές αποδοχής προκειμένου να αποτιμηθεί η λειτουργία της προσφερόμενης λύσης, σύμφωνα με τις τεχνικές προδιαγραφές τους αλλά και τις απαιτήσεις διαθεσιμότητας, απόδοσης, αξιοπιστίας, ασφάλειας και επεκτασιμότητας που έχουν οριστεί από την Αναθέτουσα Αρχή. Οι δοκιμές αποδοχής θα ολοκληρώνονται κατόπιν πιστοποίησης των αποτελεσμάτων αποδοχής από την Αναθέτουσα Αρχή. Τα false positive δεν αποτελούν ένδειξη μη ορθής λειτουργίας της λύσης.

Σε περίπτωση που κάποιες από τις εργασίες που θα πραγματοποιηθούν από τον Ανάδοχο, δύναται να προκαλέσουν την διατάραξη της ομαλής λειτουργίας (ή και διακοπή) των υφιστάμενων υπηρεσιών της ΜΟΔ Α.Ε, τότε οι εργασίες αυτές θα εκπονηθούν με τη σύμφωνη γνώμη της ΜΟΔ Α.Ε και πιθανά εκτός των εργάσιμων ωρών και ημερών μετά από σχετική απαίτηση.

Εφόσον νέες υπηρεσίες προστίθενται/ αναβαθμίζονται ή αφαιρούνται από τον Αναθέτουσα Αρχή, η παραμετροποίηση θα συνεχίζει καθ΄ όλη την διάρκεια του έργου της επιτήρησης, **χωρίς επιπλέον κόστος**. Υπεύθυνο για τον συντονισμό και την παρακολούθηση αυτών των υπηρεσιών είναι το εξειδικευμένο προσωπικό που ο Ανάδοχος θα διαθέσει στις εγκαταστάσεις της ΜΟΔ για το σύνολο της χρονικής διάρκειας του έργου.

Ειδικότερα σε ότι αφορά το σύστημα Διαχείρισης Προνομιακών Προσβάσεων, οι υπηρεσίες Εγκατάστασης και Παραμετροποίησης που θα προσφερθούν θα πρέπει να καλύπτουν το σύνολο των διαχειριστών της ΜΟΔ Α.Ε. καθώς και αριθμό εξωτερικών συνεργατών της.

Α3.2.2 Επανασχεδιασμού της υφιστάμενης αρχιτεκτονικής και των ζωνών ασφαλείας του δικτύου δεδομένων της ΜΟΔ ΑΕ.

Η απεικόνιση της νέας αρχιτεκτονικής θα γίνει στα πλαίσια της Μελέτης Εφαρμογής παράλληλα με τον καθορισμό της μεθόδου και του τρόπο υλοποίησης του έργου. Βασικός γνώμονας της νέας αρχιτεκτονικής αποτελεί η εκμετάλλευση από τον ανάδοχο στο έπακρο του εξοπλισμού και των λογισμικών που ήδη διαθέτει η Αναθέτουσα Αρχή.

Ο υφιστάμενος εξοπλισμός Next Generation firewall Fortigate 601E θα παραμείνει στο Data Center και θα χρησιμοποιηθεί ώστε να υλοποιηθεί ο λογικός διαχωρισμός του δικτύου σε εσωτερικές (Intranet) και εξωτερικές (Internet) υπηρεσίες. Οι εσωτερικές υπηρεσίες χρησιμοποιούνται από υπαλλήλους της ΜΟΔ και από υπαλλήλους άλλων υπηρεσιών συνεργαζόμενων με την ΜΟΔ. Οι εξωτερικές υπηρεσίες είναι προσβάσιμες από το Διαδίκτυο.

Για να λειτουργήσουν με ασφάλεια οι ηλεκτρονικές υπηρεσίες καθώς και για τη διευκόλυνση της διαχείρισής τους, η σχεδίαση θα βασίζεται σε αρχιτεκτονική 3 επιπέδων, η οποία θα απαρτίζεται από αποστρατιωτικοποιημένες ζώνες (De-Militarized Zones).

Οι ζώνες αυτές απαιτείται να περιλαμβάνουν υπηρεσίες παρουσίασης (presentation services – web layer) για την επικοινωνία με τον χρήστη, υπηρεσίες εφαρμογών (application services – application layer) για την υλοποίηση της επιχειρησιακής λογικής και υπηρεσίες διαχείρισης επιχειρησιακών δεδομένων, για τη διαχείριση των επιχειρησιακών δεδομένων.

Οι εργασίες επαναπρογραμματισμού και παραμετροποίησης του υφιστάμενου εξοπλισμού και λογισμικών ασφαλείας και του δικτυακού εξοπλισμού της Αναθέτουσας Αρχής θα παρέχονται από τον Ανάδοχο **χωρίς επιπλέον κόστος.**

Στα πλαίσια του επανασχεδιασμού της αρχιτεκτονικής ασφαλείας, είναι απαραίτητη και η επικαιροποίηση-επανασχεδίαση από τον Ανάδοχο της πολιτικής λήψης αντιγράφων ασφαλείας, βασιζόμενη στο νέο λογισμικό λήψης αντιγράφων ασφαλείας.

Α3.2.3 Παρακολούθησης και Διαχείρισης της Ασφαλείας του δικτύου δεδομένων 24x7 από Επιχειρησιακό Κέντρο Ασφάλειας SoC (Security Operation Center) εξοπλισμένο με την κατάλληλη πλατφόρμα SIEM (Security Information Event Management) και την κατάλληλη πλατφόρμα ανίχνευσης απειλών βασιζόμενη στην χρήση τεχνολογίας «κυβερνοπαγίδων».

Η ΜΟΔ Α.Ε επιθυμεί τη συνεχή παρακολούθηση της υποδομής της για την προστασία από κυβερνοεπιθέσεις και την ενημέρωση για πιθανά συμβάντα ασφάλειας που σχετίζονται με αυτήν σε 24ωρη βάση, για το σύνολο της διάρκειας του έργου, από Επιχειρησιακό Κέντρο Ασφάλειας (Security Operation Center) το οποίο πρέπει να βασίζεται σε ευφυής μηχανισμούς. Η λειτουργία του SoC θα γίνεται σε υποδομές εντός της Ελλάδας. Ο ανάδοχος θα έχει τον έλεγχο για τα περιστατικά ασφαλείας, με υποχρέωση την ενημέρωση της Αναθέτουσας Αρχής.

Για την υπηρεσία παρακολούθησης της ασφάλειας της υποδομής, ο Ανάδοχος θα πρέπει:

1. Να περιγράψει αναλυτικά τα δομικά χαρακτηριστικά της προτεινόμενης αρχιτεκτονικής συλλογής, επεξεργασίας και συσχέτισης δεδομένων (δικτυακή κίνηση και αρχεία καταγραφής). Επίσης θα πρέπει να περιγράφει η δυνατότητα επέκτασης της προσφερόμενης αρχιτεκτονικής σε πολλαπλά γεωγραφικά σημεία.
2. Να συγκεντρώνει σε δική του υποδομή αδιάλειπτα την πληροφορία από αρχεία καταγραφής (log files) και δικτυακών ροών (network flows).
3. Ο ανάδοχος θα πρέπει να έχει εγκατεστημένο στις υποδομές του, Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας (Security Information Event Management (SIEM) με τα απαιτούμενα χαρακτηριστικά του πίνακα συμμόρφωσης Β2.1 του Παραρτήματος ΙΙ της παρούσας διακήρυξης.
4. Το λογισμικό θα πρέπει να προσφέρει υπηρεσίες ενορχήστρωσης, αυτοματισμού και απόκρισης της ασφάλειας (SOAR) είτε με ενσωματωμένη λύση, είτε με άλλη λύση του ιδίου κατασκευαστή με τα απαιτούμενα χαρακτηριστικά του πίνακα συμμόρφωσης Β2.2 του Παραρτήματος ΙΙ της παρούσας διακήρυξης.
5. Το λογισμικό θα πρέπει να είναι σε θέση να καταγράψει δικτυακή κίνηση σε κρίσιμα σημεία της υποδομής (full packet capture), είτε με ενσωματωμένη λύση, είτε με άλλη λύση του ιδίου ή τρίτου

κατασκευαστή. Η δικτυακή κίνηση θα χρησιμοποιείται για εξακρίβωση περιστατικού, όταν αυτό απαιτείται. Επίσης θα χρησιμοποιείτε για περαιτέρω ανίχνευση απειλών. (threat hunting).

6. Να επεξεργάζεται και συσχετίζει την συγκεντρωμένη πληροφορία με στόχο την αναγνώριση πιθανών περιστατικών ασφάλειας και την κατηγοριοποίηση τους σε διαβαθμίσεις ανάλογα με την κρισιμότητά τους και τις πιθανές επιπτώσεις στην υποδομή της ΜΟΔ Α.Ε
7. Το λογισμικό θα πρέπει να κάνει χρήση τεχνικών μεγάλων δεδομένων (big data) και ελαστικότητας (elasticity) έτσι ώστε η παρεχόμενη υπηρεσία προς την Αναθέτουσα Αρχή να γίνεται με αδιάληπτο και γρήγορο τρόπο.
8. Να ενημερώνει την Αναθέτουσα Αρχή για πιθανά περιστατικά ασφάλειας σε 24ωρη βάση μέσω e-mail, ticketing system, τηλεφωνικής κλήσης ή μέσω εφαρμογής τύπου mobile application ανάλογα με την κρισιμότητά τους. Για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται ως ύψιστης κρισιμότητας και μπορεί να επιφέρουν ιδιαίτερα σημαντικές επιπτώσεις στις υποδομές της ΜΟΔ Α.Ε, απαιτείται τηλεφωνική ενημέρωση εντός 30 λεπτών από τη στιγμή εκδήλωσης του περιστατικού. Κατά την ενημέρωση για ένα περιστατικό ασφάλειας θα πρέπει να παρέχονται συμβουλές και να υλοποιούνται ενέργειες σε συνεννόηση με τα στελέχη της Αναθέτουσας Αρχής και τα στελέχη του Αναδόχου που θα βρίσκονται στις εγκαταστάσεις της ΜΟΔ, για την άμεση αντιμετώπισή του..
9. Να παραδίδει την κατάλληλη αναφορά σε τρίμηνη βάση. Η αναφορά θα περιγράφει συμβάντα που έλαβαν χώρα καθώς και προτεινόμενες βελτιστοποιήσεις με στόχο στην ασφάλεια των υπολογιστικών συστημάτων.
10. Να διατηρεί τα αρχεία καταγραφής για χρονικό διάστημα 6 μηνών κρατώντας αυτά ασφαλή και χωρίς αλλοιώσεις (integrity). Τα αρχεία καταγραφής μπορούν να αποθηκεύονται και σε χώρο που θα παραχωρήσει η Αναθέτουσα Αρχή.
11. Να συντάξει κανόνες συσχετισμού ώστε να ανιχνεύονται τυχόν κυβερνοεπιθέσεις. Σε συνεργασία με την Αναθέτουσα Αρχή θα παραμετροποιηθούν οι κανόνες ώστε να περιοριστούν τα σφάλματα (false positives), να αυξηθεί η απόδοση των κανόνων σε ασφάλεια καθώς και η διαβάθμισης των περιστατικών ασφάλειας ανάλογα με την κρισιμότητά τους.
12. Να χρησιμοποιεί σύγχρονες τεχνολογίες για ανίχνευση απειλής. Οπωσδήποτε να περιλαμβάνει χαρακτηριστικά ανίχνευσης συμπεριφοράς χρήστη, απόκλισης από συγκεκριμένα πρότυπα (δικά του και του οργανισμού) και Threat Intelligence. Να γίνει αναφορά του τρόπου παροχής της υπηρεσίας Threat Intelligence.
13. Ειδικότερα απαιτείται ο ανάδοχος να διαθέτει εγκατεστημένη στις υποδομές του, πλατφόρμα ανίχνευσης απειλών βασιζόμενη στην χρήση τεχνολογίας «κυβερνοπαγίδων». Μέσω της συγκεκριμένης πλατφόρμας θα συλλέγονται δεδομένα από τις παρεχόμενες παγίδες **κλωνοποιημένων υπηρεσιών, web εφαρμογών, συσκευών**, της Αναθέτουσας Αρχής, θα αναλύονται σε πραγματικό χρόνο και θα δημιουργούνται λίστες απειλών με όλους τους παράγοντες που σχετίζονται με πιθανή επίθεση, όπως διευθύνσεις IP, domains, file hashes ή οποιοδήποτε άλλη πληροφορία αποκτήθηκε κατά τη διάρκεια μιας επίθεσης στις παγίδες (cybertraps). Οι παραπάνω λίστες θα ενημερώνουν δυναμικά τα next generation firewalls της ΜΟΔ ,ώστε να αποτρέπεται η σύνδεση σε κακόβουλους ιστότοπους και διευθύνσεις IP.

    Τα απαιτούμενα χαρακτηριστικά της πλατφόρμας ανίχνευσης απειλών βασιζόμενη στην χρήση τεχνολογίας «κυβερνοπαγίδων» αναφέρονται αναλυτικά στον πίνακα συμμόρφωσης Β2.2 του Παραρτήματος ΙΙ της παρούσας Διακήρυξης.
14. Να προτείνει αλλαγές οι οποίες θα αυξήσουν την απόδοση της επιτήρησης.

15. Να χρησιμοποιεί τεχνολογίες συμβατές με την υποδομή της Αναθέτουσας Αρχής και το υλικό που θα χρησιμοποιηθεί να έχει υποστήριξη ορθής λειτουργίας.
16. Να ανιχνεύει σφάλματα/προβλήματα στην διαμόρφωση της υποδομής και να προτείνει λύσης διόρθωσης αυτών.
17. Η λύση που θα προσφέρει ο Ανάδοχος θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων καταγραφής κατά την αποθήκευσή τους

Στα πλαίσια παροχής υπηρεσιών Παρακολούθησης και Διαχείρισης της Ασφαλείας του δικτύου δεδομένων 24x7 ο ανάδοχος θα πρέπει:

- Να προτείνει και να υλοποιήσει μεθοδολογία ανίχνευσης ευπαθειών του εξοπλισμού. Η αποτίμηση θα πρέπει να επεξεργάζεται από τον Ανάδοχο για τον περιορισμό σφαλμάτων (false positives). Η Αναφορά αποτίμησης θα αποδίδεται στον φορέα σε τρίμηνη βάση και θα περιλαμβάνει πλήρη λίστα των ευπαθειών που εντοπίστηκαν καθώς και τα προτεινόμενα βήματα διόρθωσής τους.

  Η ανίχνευση ευπαθειών δεν θα πρέπει να επηρεάζει αισθητά την απόδοση και λειτουργία του δικτύου κατά τις παραγωγικές του ώρες. Ο ανάδοχος πριν την εφαρμογή κάθε ελέγχου θα πρέπει να εκτιμήσει την επίπτωση στην προς δοκιμή υποδομή. Οι έλεγχοι θα συνεχίσουν εφόσον κριθεί πως κάθε τμήμα της υποδομής που θα βρεθεί υπό δοκιμή θα παραμείνει λειτουργικό. Το προσωπικό της εν λόγω υπηρεσίας ή ο επικεφαλής της ομάδας θα πρέπει να είναι πιστοποιημένοι.

- Να εντοπίζει πιθανά κενά ασφαλείας σε υποδομή εξομοιώνοντας ρεαλιστικές κυβερνοεπιθέσεις, αξιοποιώντας τα αποτελέσματα της αποτίμησης ευπαθειών. Η εν λόγω υπηρεσία θα αφορά την κεντρική υποδομή της Αναθέτουσας Αρχής και θα παρέχεται εξαμηνιαίως. Τα εργαλεία που θα χρησιμοποιηθούν θα πρέπει να είναι διεθνώς πιστοποιημένων κατασκευαστών ή εργαλεία του Αναδόχου. Χρειάζεται πλήρη συμφωνία για την ημερομηνία διεξαγωγής του ελέγχου καθώς και ρητή έγκριση από την Αναθέτουσα Αρχή για την περαιτέρω εκμετάλλευση αδυναμιών (exploitation). Αναλυτικά χαρακτηριστικά των υπηρεσιών Ανίχνευσης Ευπαθειών αναφέρονται στον πίνακα συμμόρφωσης Β1.2

Α3.2.4 Υποστηρικτικές δράσεις Έργου

Ο ανάδοχος θα παρέχει στις **εγκαταστάσεις της ΜΟΔ σε καθημερινή βάση και για το σύνολο της διάρκειας του έργου, εξειδικευμένο προσωπικό αποτελούμενο από τουλάχιστον 2 στελέχη**. Το εν λόγω προσωπικό θα αναλάβει την διαχείριση των υφιστάμενων και υπό προμήθεια συσκευών και λογισμικών ασφάλειας καθώς και του συνόλου των δικτυακών συσκευών του δικτύου δεδομένων της ΜΟΔ. Τα παραπάνω στελέχη θα λειτουργούν επικουρικά στον εσωτερικό Υ.Α.Σ.Π.Ε. (Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών) όπως έχει οριστεί από την εταιρία, διασφαλίζοντας ότι η ΜΟΔ διατηρεί την κατάλληλη ορατότητα και τον αναγκαίο έλεγχο επί της ασφάλειας των συστημάτων πληροφορικής και επικοινωνιών. Παράλληλα θα αποτελούν το σημείο επαφής με τα στελέχη του αναδόχου που λειτουργούν το SoC και θα υλοποιούν από κοινού τις απαραίτητες ενέργειες για την αντιμετώπιση των δικτυακών απειλών και των πιθανών κυβερνοεπιθέσεων.

Επίσης το εν λόγω προσωπικό θα αναλάβει την υλοποίηση και την παρακολούθηση της διαδικασίας λήψης αντιγράφων ασφαλείας για 200 εικονικούς εξυπηρετητές με την χρήση του νέου λογισμικού λήψης αντιγράφων ασφαλείας.

Α3.2.5 Υπηρεσίες Εκπαίδευσης

Ο ανάδοχος στο πλαίσιο του έργου θα παρέχει υπηρεσίες εκπαίδευσης, ειδικότερα:

- Εκπαίδευση του αρμόδιου προσωπικού της Αναθέτουσας Αρχής στον προσφερόμενο προς εγκατάσταση στο Πληροφοριακό Κέντρο της Αναθέτουσας Αρχής εξοπλισμό και λογισμικό.

- Εκπαίδευση του αρμόδιου προσωπικού της Αναθέτουσας Αρχής πριν την έναρξη της υπηρεσίας Παρακολούθησης και Διαχείρισης της Ασφαλείας του δικτύου δεδομένων.
- Διεξαγωγή σεμιναρίων τεχνικής κατάρτισης για την σωστή συνεργασία και αποτελεσματική απόκριση σε περιστατικά ασφάλειας.
- Εκπαιδευτικό υλικό για τις απαραίτητες γνώσεις και δεξιότητες.

Οι υποψήφιοι Ανάδοχοι, κατά την πρόταση τους, θα πρέπει να υποβάλουν «Πλάνο Εκπαίδευσης» στο οποίο θα περιγράφονται αναλυτικά οι προτεινόμενες υπηρεσίες εκπαίδευσης και στο οποίο θα αναφέρονται: η μεθοδολογία και οι τεχνικές που θα ακολουθήσουν για την οργάνωση της εκπαίδευσης, οι ώρες εκπαίδευσης σεμιναρίων που θα προσφερθούν, ενδεικτικά περιεχόμενα της εκπαίδευσης, το εκπαιδευτικό και εποπτικό υλικό που θα προσφερθεί (σε έντυπη ή ηλεκτρονική μορφή) και κάθε άλλο στοιχείο που μπορεί να ληφθεί υπόψη από την Αναθέτουσα Αρχή κατά την αξιολόγηση. Η εκπαίδευση θα πραγματοποιηθεί στις κεντρικές εγκαταστάσεις της Αναθέτουσας Αρχής, κατά τις εργάσιμες ημέρες και ώρες.

Α3.2.6 Παροχή Υπηρεσιών υποστήριξης του Υπευθύνου Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών (Υ.Α.Σ.Π.Ε.)

Ο ανάδοχος οφείλει να παρέχει υπηρεσίες υποστήριξης στο ρόλο του Υ.Α.Σ.Π.Ε. διασφαλίζοντας ότι η ΜΟΔ διατηρεί την κατάλληλη ορατότητα και τον αναγκαίο έλεγχο επί της ασφάλειας των συστημάτων πληροφορικής και επικοινωνιών. Αυτό περιλαμβάνει την εποπτεία της εφαρμογής μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας, την παρακολούθηση της ενιαίας πολιτικής κυβερνοασφάλειας και τη διασφάλιση ότι η συμμόρφωση με τις υποχρεώσεις αναφοράς περιστατικών είναι έγκαιρη, ακριβής και πλήρης.

Σύμφωνα με την Υπουργική Απόφαση 1899/2025, ο Υ.Α.Σ.Π.Ε. εποπτεύει, επιμελείται και συντονίζει τα εξής:

- Την εποπτεία της ασφάλειας δικτύων και συστημάτων πληροφορικής, διασφαλίζοντας ότι οι πολιτικές, οι έλεγχοι και τα μέτρα διαχείρισης κινδύνων εφαρμόζονται με συνέπεια.
- Τη λειτουργία ως επίσημος σύνδεσμος με την Εθνική Αρχή Κυβερνοασφάλειας (ΕΝCA) και άλλες αρμόδιες αρχές, συντονίζοντας την αναφορά περιστατικών και τις ρυθμιστικές επικοινωνίες.
- Την εποπτεία της ενιαίας πολιτικής κυβερνοασφάλειας, του μητρώου περιουσιακών στοιχείων ΤΠΕ, της ασφάλειας της εφοδιαστικής αλυσίδας και της διακυβέρνησης επιχειρησιακής συνέχειας.
- Την παροχή ανεξάρτητης αναφοράς για κινδύνους και απειλές κυβερνοασφάλειας προς την ανώτατη διοίκηση, εξασφαλίζοντας ορατότητα σε επίπεδο Διοικητικού Συμβουλίου.
- Την εποπτεία προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και της συμμετοχής του οργανισμού σε επαγγελματικά fora και ενώσεις.
- Τη διατήρηση ανεξαρτησίας, εμπιστευτικότητας και ουδετερότητας σε όλα τα εποπτικά καθήκοντα, αποφεύγοντας συγκρούσεις συμφερόντων και συνεργαζόμενος με τον Υπεύθυνο Προστασίας Δεδομένων (DPO) ή τις Εθνικές Αρχές Ασφαλείας όπου απαιτείται.

Στα πλαίσια υποστήριξης του Υ.Α.Σ.Π.Ε., ο Ανάδοχος θα παραδώσει στη ΜΟΔ ένα σύνολο τυποποιημένων πολιτικών κυβερνοασφάλειας, οι οποίες βασίζονται σε διεθνή πρότυπα και βέλτιστες πρακτικές (π.χ. ISO 27001, ENISA guidelines, NIS2 requirements). Οι πολιτικές αυτές καλύπτουν τους κύριους τομείς διακυβέρνησης της ασφάλειας πληροφοριών, όπως:

- Πολιτική Ασφάλειας Πληροφοριών.
- Πολιτική Διαχείρισης Κινδύνων.
- Πολιτική Διαχείρισης Περιστατικών Ασφαλείας.
- Πολιτική Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφή.
- Πολιτική Διαχείρισης Πρόσβασης και Χρήσης Συστημάτων.

Α3.2.7 Παροχή Υπηρεσιών ελέγχου διείσδυσης στο εξωτερικό και εσωτερικό περιβάλλον στις υποδομές της Αναθέτουσας Αρχής.

Ο ανάδοχος οφείλει να παρέχει υπηρεσίες ελέγχου ασφάλειας (penetration testing), με σκοπό την αξιολόγηση του επιπέδου ασφάλειας των πληροφοριακών συστημάτων της ΜΟΔ. Στόχος είναι ο εντοπισμός, η τεκμηρίωση και η προτεραιοποίηση ευπαθειών, καθώς και η πιστοποίηση της αποτελεσματικότητας των διορθωτικών ενεργειών μέσω re-testing.

Εύρος Έργου

Οι παρακάτω έλεγχοι ασφάλειας οφείλουν να εκτελούνται **τουλάχιστον μια (1) φορά ετησίως** από τον ανάδοχο:

- External Penetration Test: Έλεγχος έως 128 δημόσιων IP.
- Internal Penetration Test: Έλεγχος έως 250 εσωτερικών συσκευών/συστημάτων.

Μεθοδολογίες εκτέλεσης

Κατά την εκτέλεση του External Penetration Test ο ανάδοχος υποχρεούται να ακολουθήσει τουλάχιστον τα ακόλουθα στάδια:

Passive Information Gathering:

- Συλλογή πληροφοριών από δημόσιες πηγές (OSINT) χωρίς ενεργή επαφή με την υποδομή της ΜΟΔ.
- Τεκμηρίωση πηγών και ευρημάτων.

Active Information Gathering:

- Ενεργά probes για αναγνώριση hosts, υπηρεσιών, εκδόσεων λογισμικού, firewall/IDS/IPS signatures, κ.λπ.
- OS fingerprinting, port scanning, banner grabbing.

Vulnerability Mapping:

- Συγκέντρωση και ταξινόμηση των πληροφοριών.
- Δημιουργία χάρτη ευπαθειών και επιλογή στρατηγικής για exploitation (εργαλεία, payloads, sequence).

Exploitation:

- Εφαρμογή επιθέσεων (μεμονωμένων και συνδυαστικών) για την επαλήθευση των ευπαθειών και την εκτίμηση του πραγματικού αντίκτυπου για τη ΜΟΔ.
- Τεκμηρίωση επιτυχημένων break-ins και εκτίμηση πιθανών ζημιών.
- Κατά τη φάση αυτή να παρακολουθείται σχετικό traffic (sniffing) όπου απαιτείται και όπου επιτρέπεται.

Re-Testing:

- Επαναληπτικός έλεγχος μετά από διορθωτικές ενέργειες για επαλήθευση αποτελεσματικότητας.

Κατά την εκτέλεση του Internal Penetration Test ο ανάδοχος υποχρεούται να ακολουθήσει τουλάχιστον τα ακόλουθα στάδια:

Active Information Gathering:

- Ενεργά probes εντός δικτύου για χαρτογράφηση συσκευών, υπηρεσιών, εκδόσεων, κ.λπ.

Vulnerability Mapping:

- Συγκέντρωση, ταξινόμηση και δημιουργία χάρτη διαδρομών εκμετάλλευσης.

Exploitation:

- Συνδυαστική εκμετάλλευση ευπαθειών (lateral movement, privilege escalation, persistence) για προσομοίωση πραγματικών εσωτερικών επιθέσεων.
- Παρακολούθηση δικτυακής κίνησης για ανεύρεση ευαίσθητων δεδομένων όπου επιτρέπεται.

Re-Testing:

- Επανάληψη ελέγχων μετά από διορθωτικές ενέργειες.

Απαιτούμενα Εργαλεία & Τεχνικές

Κατά την εκτέλεση των ελέγχων ο ανάδοχος οφείλει να χρησιμοποιήσει εργαλεία για: Network/Infrastructure, Web applications, Databases, Password auditing, OSINT, Exploitation.

Ενδεικτική λίστα εργαλείων: Kali Linux tools, Burp Suite, John the Ripper, Maltego, Telerik Fiddler, Metasploit, Tenable Nessus, Nmap, Nikto, OWASP ZAP, Sqlmap, w3af, DirBuster, DalFox.

Ο ανάδοχος δύναται να χρησιμοποιήσει ισοδύναμα εργαλεία με τεκμηρίωση.

Παραδοτέα

Τα αποτελέσματα του έργου θα συνοψίζονται από τον ανάδοχο σε γραπτή αναφορά (Written Report) και θα παρουσιάζονται σε Executive Presentation προς τη Διοίκηση της ΜΟΔ. Η αναφορά οφείλει να περιλαμβάνει τα εξής τμήματα:

- Introduction, Scope & Approach: Περιγραφή σκοπού του penetration test, πεδίου εφαρμογής και μεθοδολογίας.
- Executive Summary: Εκτελεστική σύνοψη των ευρημάτων και σχετικών γραφημάτων (κατηγοριοποίηση κινδύνου ευπαθειών) και σημεία βελτίωσης για τα υφιστάμενα μέτρα ασφαλείας.
- Findings Summary: Συνοπτική παρουσίαση των πιο κρίσιμων ευρημάτων.
- Consolidated Solution/Correction Plan: Ενοποιημένο σχέδιο διόρθωσης/μείωσης των ευπαθειών.
- Security Control Areas: Συσχέτιση των περιοχών ασφάλειας με τις εντοπισθείσες ευπάθειες.
- Findings and Observations: Αναλυτικά στοιχεία για κάθε ευπάθεια (Target, DNS Name, Operating System, Web Technologies, Network Port, Affected Page/Service, Vulnerability Name, Severity, Description, Impact, Recommendation, Key Recommendation, Recommendation Rating).
- Evidence: Παροχή τεχνικών αποδεικτικών στοιχείων.

Επιπλέον του παραδοτέου σε μορφή PDF που περιγράφεται παραπάνω, ο ανάδοχος οφείλει να παραδώσει και κατάλογο ευρημάτων σε μορφή Excel για ευκολότερη διαχείριση και παρακολούθηση κινδύνου.

Α3.2.7 Άλλες Υπηρεσίες

Οι υποψήφιοι Ανάδοχοι ενθαρρύνονται να περιγράψουν τυχόν επιπλέον υπηρεσίες οι οποίες κρίνονται αναγκαίες για την επιτυχή ολοκλήρωση του έργου και οι οποίες δεν έχουν προβλεφθεί στην προκήρυξη.

Σε κάθε περίπτωση, για τις επιπλέον υπηρεσίες θα πρέπει να αιτιολογηθεί η ανάγκη για την παροχή τους, η ωφέλεια για την ΜΟΔ Α.Ε, καθώς και η φάση του έργου στην οποία πρόκειται να προσφερθούν.

Το σύνολο των παραπάνω υπηρεσιών θα προσφέρεται **χωρίς κόστος.**

Α4 Διάρκεια Έργου – Χρονοδιάγραμμα Υλοποίησης

Η διάρκεια της Σύμβασης ορίζεται σε **τρία (3) έτη από την υπογραφή της**.

ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΥΛΟΠΟΙΗΣΗΣ ΕΡΓΟΥ														
Α/Α	Περιγραφή Εργασίας	Μήνες	1				2				3 Έως 36			
		Εβδομάδες	1	2	3	4	5	6	7	8	9 έως 156			
ΠΡΟΜΗΘΕΙΑ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ ΕΞΟΠΛΙΣΜΟΥ & ΛΟΓΙΣΜΙΚΩΝ														
1	Μελέτη Εφαρμογής													
2	Παραγγελία Εξοπλισμού													
3	Καθορισμός ομάδων εγκατάτασης και παραμετροποίησης													
4	Ανάλυση και προετοιμασία χώρων εγκατάστασης													
5	Παραλαβη εξοπλισμού													
6	Φυσική εγκατάσταση εξοπλισμού και λογισμικών													
7	Παραμετροποίηση υφιστάμεων συστημάτων σύμφωνα με την νέα αρχιτεκτονική													
8	Διασύνδεση νέων και υφιστάμενων συστημάτων με SOC													
9	Παραμετροποίηση νέου εξοπλισμού και λογισμικών													
ΥΠΗΡΕΣΙΕΣ														
10	Εκπαίδευση													
11	Υπηρεσίες καθημερινής υποστήριξης για 3 χρόνια													
12	Υπηρεσίες παρακολούθησης και διαχείρισης της ασφάλειας του δικτύου δεδομένων 24x7 από SOC για 3 χρόνια													
13	Υπηρεσίες ανίχνευσης και αποτίμησης ευπαθειών													
14	Ενδεχόμενες λοιπές υπηρεσίες													

Α5 Ομάδα Έργου/Σχήμα Διοίκησης της Σύμβασης

Α5.1 Ομάδα Έργου Αναδόχου

Η Αναθέτουσα Αρχή θα έχει την κύρια ευθύνη επίβλεψης και ελέγχου της πορείας ανάπτυξης και υλοποίησης του έργου, ενώ την κύρια ευθύνη υλοποίησης του έργου την έχει ο ανάδοχος.

Ο ανάδοχος υποχρεούται να υποβάλλει στην προσφορά του (στον φάκελο "ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ") ολοκληρωμένη πρόταση για το σχήμα διοίκησης, την οργάνωση και τον προγραμματισμό του έργου, το προσωπικό που θα διαθέσει για τη διοίκηση και υλοποίηση του έργου. Τυχόν αλλαγή του προσωπικού θα τελεί υπό την έγκριση της Αναθέτουσας Αρχής, κατόπιν γνωμοδοτήσεως της αρμόδιας Επιτροπής Παραλαβής (ΕΠ).

Ο υποψήφιος ανάδοχος πρέπει να διαθέτει Ομάδα Έργου με στελέχη επαρκή σε πλήθος και ικανότητες για την ανάληψη του έργου, η οποία να αποτελείται κατ' ελάχιστον από:

- Έναν (1) υπεύθυνο έργου, ο οποίος θα πρέπει να διαθέτει πτυχίο ανώτατης εκπαίδευσης στον κλάδο Μηχανικής / Πληροφορικής, μεταπτυχιακό MBA και συνολική επαγγελματική εμπειρία τουλάχιστον είκοσι (20) ετών.
- Έναν (1) αναπληρωτή Υπεύθυνο Έργου, ο οποίος θα πρέπει να διαθέτει πτυχίο ανώτατης εκπαίδευσης στον κλάδο Πληροφορικής και συνολική επαγγελματική εμπειρία τουλάχιστον δέκα πέντε (15) ετών
- Έναν (1) Υπεύθυνο Ποιότητας Έργου, ο οποίος θα πρέπει να διαθέτει πτυχίο ανώτατης εκπαίδευσης και επαγγελματική εμπειρία τουλάχιστον δεκαπέντε (15) ετών
- Έναν (1) Ειδικό Κυβερνοασφάλειας, ο οποίος να διαθέτει πτυχίο θετικών επιστημών και τουλάχιστον 20ετή επαγγελματική εμπειρία στην ασφάλεια πληροφοριακών συστημάτων
- Έναν (1) Ειδικό Κυβερνοασφάλειας, ο οποίος να διαθέτει τουλάχιστον 10ετή επαγγελματική εμπειρία στην ασφάλεια πληροφοριακών συστημάτων και συγκεκριμένα στην υλοποίηση λύσεων Web Application Firewall (WAF)

- Έναν (1) Μηχανικό Κυβερνοασφάλειας, ο οποίος να διαθέτει τουλάχιστον 5ετή επαγγελματική εμπειρία στην ασφάλεια πληροφοριακών συστημάτων και συγκεκριμένα στην υλοποίηση λύσεων Privileged Access Management (PAM)
- Έναν (1) Μηχανικό Κυβερνοασφάλειας, ο οποίος να διαθέτει πτυχίο Πληροφορικής και τουλάχιστον 3ετή επαγγελματική εμπειρία στην ασφάλεια πληροφοριακών συστημάτων. Επίσης, θα πρέπει να διαθέτει τουλάχιστον μία (1) πιστοποίηση κατά των προσφερόμενο κατασκευαστή των προτεινόμενων λύσεων περιμέτρου.
- Έναν (1) Μηχανικό Κυβερνοασφάλειας, ο οποίος θα πρέπει να διαθέτει πτυχίο ανώτατης εκπαίδευσης στον κλάδο Πληροφορικής και συνολική επαγγελματική εμπειρία τουλάχιστον δέκα (10) ετών.
- Έναν (1) Μηχανικό Κυβερνοασφάλειας, ο οποίος θα πρέπει να διαθέτει πτυχίο ανώτατης εκπαίδευσης στον κλάδο Πληροφορικής και συνολική επαγγελματική εμπειρία τουλάχιστον δέκα (10) ετών σε αντίστοιχα έργα Επιχειρησιακού Κέντρου Ασφάλειας (Security Operation Center).
- Δύο (2) Αναλυτές Κυβερνοασφάλειας, οι οποίοι θα πρέπει να διαθέτουν πτυχίο ανώτατης εκπαίδευσης στον κλάδο Πληροφορικής και συνολική επαγγελματική εμπειρία τουλάχιστον δέκα (10) ετών σε αντίστοιχα έργα Επιχειρησιακού Κέντρου Ασφάλειας (Security Operation Center)
- Δέκα (10) άτομα Τεχνικούς, οι οποίοι θα πρέπει να διαθέτουν πτυχίο ανώτερης/ανώτατης εκπαίδευσης και επαγγελματική εμπειρία τουλάχιστον τριών (3) ετών έκαστος.

Σε περίπτωση ένωσης οικονομικών φορέων, οι παραπάνω ελάχιστες απαιτήσεις πρέπει να καλύπτονται αθροιστικά από τα μέλη της ένωσης.

Α5.2 Επιτροπή Παραλαβής της Αναθέτουσας Αρχής

Το έργο θα το παρακολουθεί και θα το διαχειρίζεται η Επιτροπή Παραλαβής (ΕΠ), η οποία θα συσταθεί σύμφωνα με τον ν. 4412/2016 και θα αποτελείται από στελέχη της Αναθέτουσας Αρχής. Η ΕΠ θα διαχειρίζεται όλες τις διαστάσεις του Έργου και θα ενημερώνει την διοίκηση της Αναθέτουσας Αρχής για την πορεία του. Η ΕΠ θα έχει τη εποπτεία της πορείας των εργασιών και των συμβατικών υποχρεώσεων του Αναδόχου και θα είναι αρμόδια για την παραλαβή και πιστοποίηση όλων των παραδοτέων, καθώς και την σύνταξη των αντιστοίχων κατά περίπτωση πρωτοκόλλων.

Α6 Τόπος υλοποίησης/παράδοσης

Ο Ανάδοχος θα πρέπει να εγκαταστήσει και να παραδώσει σε πλήρη λειτουργία το σύνολο του ζητούμενου εξοπλισμού και λογισμικού.

Η παράδοση και εγκατάσταση του εξοπλισμού θα γίνει στις εγκαταστάσεις της Αναθέτουσας Αρχής.

Α7 Εγγύηση Εξοπλισμού

Το σύνολο του υπό προμήθεια **εξοπλισμού** απαιτείται να καλύπτεται από **Εγγύηση Κατασκευαστή διάρκειας τουλάχιστον 5 (πέντε) ετών χωρίς επιπλέον κόστος**, συμπεριλαμβανομένων και των αδειών χρήσης. Αντίστοιχα, το σύνολο του υπό προμήθεια **λογισμικού** απαιτείται να συνοδεύεται από **ενεργή άδεια χρήσης για τα επόμενα 5 (πέντε) χρόνια**.

Ειδικά για το υπό προμήθεια λογισμικό ο ανάδοχος παρέχει υπηρεσίες αναβάθμισης, σε περίπτωση νέων εκδόσεων του λογισμικού που χρησιμοποιείται, κατόπιν συνεννόησης με την Αναθέτουσα Αρχή και εφόσον δεν προκαλείται κάποια δυσλειτουργία λόγω ασυμβατότητας εκδόσεων, σε οποιοδήποτε χρονικό σημείο και για όλο το χρονικό διάστημα της διάρκειας της σύμβασης.

Ο ανάδοχος αναλαμβάνει την υποχρέωση να αντικαθιστά, διορθώνει, τροποποιεί το υλικό ή λογισμικό που δυσχεραίνει την εύρυθμη και αξιόπιστη λειτουργία του συστήματος, τηρώντας ενήμερη την Αναθέτουσα Αρχή.

Ο ανάδοχος είναι υποχρεωμένος να παρέχει τεχνική υποστήριξη για όλο το χρονικό διάστημα της εγγύησης καλής λειτουργίας. Οι αναλυτικοί όροι της τεχνικής υποστήριξης αναφέρονται στο πίνακα συμμόρφωσης Β1.

Η μη έγκαιρη και αποτελεσματική παροχή τεχνικής υποστήριξης, η μη διάθεση των αιτουμένων ανταλλακτικών εντός του καθοριζόμενου χρονικού ορίου, καθώς και η καταστρατήγηση των λοιπών όρων της συμβάσεως εκ μέρους του αναδόχου, θα αποτελούν λόγο επιβολής των προβλεπόμενων κυρώσεων.

Για όλα τα προϊόντα λογισμικού που θα προσφερθούν, να περιέρχονται όλες οι άδειες χρήσης αυτών στην αρμόδια υπηρεσία, η οποία και αποκτά τη νομιμότητα της χρήσης τους χωρίς κανένα περιορισμό.

ΠΑΡΑΡΤΗΜΑ ΙΙ – ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ

Ο υποψήφιος Ανάδοχος, συμπεριλαμβάνει στον φάκελο «Τεχνική Προσφορά», επί ποινή αποκλεισμού, τρία (3) ευδιάκριτα τμήματα που ακολουθούν την διάρθρωση:

- ΤΜΗΜΑ Ι – ΤΕΚΜΗΡΙΩΣΗ ΚΑΤΑΝΟΗΣΗΣ ΤΟΥ ΠΕΡΙΒΑΛΛΟΝΤΟΣ ΤΟΥ ΕΡΓΟΥ
    - Τεχνολογικό περιβάλλον του έργου
    - Λειτουργικό & επιχειρησιακό περιβάλλον του έργου
    - Πλάνο εκπαίδευσης
- ΤΜΗΜΑ ΙΙ – ΟΡΓΑΝΩΣΗ ΟΜΑΔΑΣ ΕΡΓΟΥ (παρ. Α5.1 του Παραρτήματος Ι)
    - Σχήμα διοίκησης και υλοποίησης
    - Εξειδίκευση και συμπληρωματικότητα των μελών της ομάδας έργου
        - Τεκμηρίωση - περιγραφή σχετικών δεξιοτήτων
        - Βιογραφικά σημειώματα
- ΤΜΗΜΑ ΙΙΙ – ΠΙΝΑΚΕΣ ΣΥΜΜΟΡΦΩΣΗΣ

Στη συνέχεια παρατίθενται τα απαιτητά και επιθυμητά τεχνικά χαρακτηριστικά του υπό προμήθεια Εξοπλισμού. Ο υποψήφιος Ανάδοχος υποχρεούται να υποβάλλει στην προσφορά του (στον φάκελο «ΤΕΧΝΙΚΗ ΠΡΟΣΦΟΡΑ») συμπληρωμένους τους κατωτέρω Πίνακες Συμμόρφωσης, σύμφωνα με τα παρακάτω:

Στη Στήλη «ΠΡΟΔΙΑΓΡΑΦΗ», περιγράφονται αναλυτικά οι αντίστοιχοι τεχνικοί όροι, υποχρεώσεις ή επεξηγήσεις για τα οποία θα πρέπει να δοθούν αντίστοιχες απαντήσεις.

Αν στη στήλη «ΑΠΑΙΤΗΣΗ» έχει συμπληρωθεί η λέξη «ΝΑΙ» ή ένας αριθμός (που σημαίνει υποχρεωτικό αριθμητικό μέγεθος της προδιαγραφής και απαιτεί συμμόρφωση), τότε η αντίστοιχη προδιαγραφή είναι υποχρεωτική για τον υποψήφιο Ανάδοχο, θεωρούμενη ως απαράβατος όρος σύμφωνα με την παρούσα Διακήρυξη. Προσφορές που δεν καλύπτουν πλήρως απαράβατους όρους απορρίπτονται ως απαράδεκτες.

Στη στήλη «ΑΠΑΝΤΗΣΗ» σημειώνεται η απάντηση του Αναδόχου που έχει τη μορφή ΝΑΙ/ΟΧΙ εάν η αντίστοιχη προδιαγραφή πληρούται ή όχι από την Προσφορά ή ένα αριθμητικό μέγεθος που δηλώνει την ποσότητα του αντίστοιχου χαρακτηριστικού στην Προσφορά. Απλή κατάφαση ή επεξήγηση δεν αποτελεί απόδειξη πλήρωσης της προδιαγραφής και η αρμόδια Επιτροπή έχει την υποχρέωση ελέγχου και επιβεβαίωσης της πλήρωσης της απαίτησης.

Στη στήλη «ΠΑΡΑΠΟΜΠΗ» θα καταγραφεί η σαφής παραπομπή σε Παράρτημα της Τεχνικής Προσφοράς, το οποίο θα περιλαμβάνει αριθμημένα Τεχνικά Φυλλάδια κατασκευαστών ή αναλυτικές τεχνικές περιγραφές των υπηρεσιών, του εξοπλισμού ή του τρόπου διασύνδεσης και λειτουργίας ή αναφορές μεθοδολογίας εγκατάστασης και υποστήριξης κλπ., που κατά την κρίση του υποψηφίου Αναδόχου τεκμηριώνουν τα στοιχεία των Πινάκων Συμμόρφωσης.

Τονίζεται ότι είναι υποχρεωτική η απάντηση σε όλα τα σημεία των ΠΙΝΑΚΩΝ ΣΥΜΜΟΡΦΩΣΗΣ και η παροχή όλων των πληροφοριών που ζητούνται.

Η αρμόδια Επιτροπή θα αξιολογήσει τα παρεχόμενα από τους υποψήφιους Αναδόχους στοιχεία κατά τον έλεγχο των Τεχνικών Προσφορών.

Σε περίπτωση που δεν έχει συμπληρωθεί η στήλη «ΑΠΑΝΤΗΣΗ», για έστω και ένα από τους όρους στον πίνακα συμμόρφωσης, τότε θεωρείται ότι δεν υπάρχει απάντηση στο σχετικό όρο. Η Επιτροπή Αξιολόγησης Προσφορών δύναται να ζητήσει εγγράφως από τους υποψηφίους Αναδόχους παρουσίαση της προσφερόμενης λύσης για το παρόν έργο.

Α Εξοπλισμός – Λογισμικά

1. Next Generation Firewall

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1	**Γενικά Χαρακτηριστικά**			
1.1.1	Να αναφερθεί ο κατασκευαστής και το μοντέλο	ΝΑΙ		
1.1.2	Απαιτούμενος αριθμός τεμαχίων	2		
1.1.3	USB Θύρες	≥ 2		
1.1.4	Θύρες management GE RJ45	≥ 1		
1.1.5	Θύρες GE SFP	≥ 8		
1.1.6	Θύρες 10 GE SFP+	≥ 4		
1.1.7	Θύρες 25 GE SFP28	≥ 4		
1.1.8	Λειτουργία σε διάταξη υψηλής διαθεσιμότητας (clustering) active-active και active-standby. Να περιγραφούν αναλυτικά οι σχετικές αρχιτεκτονικές υψηλής διαθεσιμότητας.	ΝΑΙ		
1.1.9	Δυνατότητα προσθήκης επί πλέον συσκευών σε διάταξη υψηλής διαθεσιμότητας και λειτουργία active-active ή active-standby. Να αναφερθεί ο μέγιστος αριθμός υποστηριζόμενων συσκευών σε λειτουργία υψηλής διαθεσιμότητας.	ΕΠΙΘΥΜΗΤΟ		
1.1.10	Κατακερματισμός σε πολλά λογικά τείχη προστασίας (virtual firewall)	ΝΑΙ		
1.1.11	Να αναφερθεί η μέγιστη δυνατότητα υποστήριξης λογικών τειχών προστασίας χωρίς να απαιτείται επιπλέον άδεια.	≥ 10		
1.1.12	Ενσωματωμένη υποστήριξη IPS, antivirus και application control.	ΝΑΙ		
1.1.13	Ενσωματωμένη υποστήριξη προστασίας σε Denial of Service (DoS)	ΝΑΙ		
1.1.14	Τοποθέτηση σε Rack	≥ 1RU		
1.1.15	Να προσφερθούν όλα τα απαραίτητα υλικά ανάρτησης.	ΝΑΙ		
1.2	**Επιδόσεις**			
1.2.1	Firewall throughput σε IPv4 και IPv6 (για μέγεθος πακέτου 512-byte και κίνηση UDP)	≥ 150 Gbps		
1.2.2	Ταυτόχρονες TCP συνδέσεις	≥ 15 Million		
1.2.3	Ρυθμός αποκατάστασης νέων TCP συνδέσεων ανά δευτερόλεπτο	≥ 700,000		
1.2.4	IPS throughput (enterprise mix)	≥ 40 Gbps		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.2.5	NGFW (IPS+Firewall+Application control) throughput (enterprise mix)	≥ 30 Gbps		
1.2.6	IPsec VPN throughput	≥ 50 Gbps		
1.2.7	SSL VPN throughput	≥ 9 Gbps		
1.2.8	Threat Protection (IPS+Firewall+Application control+Malware protection) throughput (enterprise mix)	≥ 25 Gbps		
1.2.9	SSL inspection throughput	≥ 15 Gbps		
1.2.10	Να αναφερθούν οι πιστοποιήσεις που έχει λάβει η λύση από ανεξάρτητους οίκους αξιολόγησης	ΝΑΙ		
1.3	**Υποστήριξη L2 και L3**			
1.3.1	Υποστήριξη VLAN IEEE 802.1q	ΝΑΙ		
1.3.2	Υποστήριξη link aggregation IEEE 802.3ad	ΝΑΙ		
1.3.3	Υποστήριξη IPv4 και IPv6	ΝΑΙ		
1.3.4	Υποστήριξη OSPF v.2 και v.3	ΝΑΙ		
1.3.5	Υποστήριξη BGP v.4+	ΝΑΙ		
1.3.6	Υποστήριξη policy routing	ΝΑΙ		
1.3.7	Υποστήριξη NTP	ΝΑΙ		
1.3.8	Υποστήριξη DHCP server/relay	ΝΑΙ		
1.4	**Πολιτικές ασφαλείας**			
1.4.1	Η υπηρεσία antivirus θα πρέπει να υποστηρίζει: - Virus signature database scan. - Grayware scan. - Heuristics scan.	ΝΑΙ		
1.4.2	Δυνατότητα αποστολής των ύποπτων αρχείων σε περιβάλλον Hardware Sandbox.	ΝΑΙ		
1.4.3	Η λειτουργία IPS θα πρέπει να υποστηρίζει δημιουργία custom υπογραφών από τον διαχειριστή.	ΝΑΙ		
1.4.4	Υποστήριξη web filtering	ΝΑΙ		
1.4.5	Υποστήριξη SSL inspection	ΝΑΙ		
1.5	**Διαχείριση**			
1.5.1	Διαχείριση μέσω γραμμής εντολής (CLI)	ΝΑΙ		
1.5.2	Διαχείριση μέσω ενσωματωμένου γραφικού περιβάλλοντος (GUI)	ΝΑΙ		
1.5.3	Πρόσβαση διαχειριστών μέσω HTTPS και SSH	ΝΑΙ		
1.5.4	Υποστήριξη SNMP v.1, 2c και 3	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.5.5	Δημιουργία πολιτικής password και επιβολή συμμόρφωσης σε αυτή. Η πολιτική password θα πρέπει να υποστηρίζει υποχρεωτικά τα εξής: - Ελάχιστο μήκος password - Υποχρεωτικά κεφαλαία/μικρά γράμματα - Υποχρεωτική χρήση μη αλφαριθμητικών χαρακτήρων - Υποχρεωτική χρήση αριθμών - Χρονική διάρκεια password - Μη επανάληψη ίδιου password	ΝΑΙ		
1.5.6	Υποστήριξη RADIUS και LDAP	ΝΑΙ		
1.5.7	Δυνατότητα ενοποίησης με πλατφόρμα κεντρικής διαχείρισης κατά προτίμηση του ίδιου κατασκευαστη.	ΕΠΙΘΥΜΗΤΟ		
1.6	**Υπηρεσίες Υποστήριξης**			
1.6.1	Ο εξοπλισμός θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 διάρκειας πέντε (5) ετών. Οι παραπάνω υπηρεσίες θα πρέπει να περιλαμβάνουν: • Τηλεφωνική υποστήριξη 24x7 • Δυνατότητα επίλυσης τεχνικών προβλημάτων μέσω δημιουργίας ticket • Αντικατάσταση του εξοπλισμού σε περίπτωση βλάβης πριν την αποστολή του χαλασμένου • Service και ανταλλακτικά στο εξουσιοδοτημένο επισκευαστικό κέντρο του κατασκευαστή	ΝΑΙ		
1.6.2	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη της λειτουργίας antivirus και IPS και web filtering διάρκειας πέντε (5) ετών.	ΝΑΙ		
1.6.3	Θα πρέπει να προσφερθούν όλες οι επίπλεον άδειες χρήσης που τυχόν απαιτούνται για την υποστήριξη όλων των λειτουργικών χαρακτηριστικών των πινάκων 1.1 έως και 1.5 διάρκειας (5) ετών, σε περίπτωση που αυτά δεν καλύπτονται από τις άδειες του σημείου. 1.6.2.	ΝΑΙ		

2. Web Application Firewall (WAF)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.1	**Γενικά Χαρακτηριστικά**			
2.1.1	Να αναφερθεί ο κατασκευαστής και το μοντέλο	ΝΑΙ		
2.1.2	Απαιτούμενος αριθμός τεμαχίων	**1**		
2.1.3	Το προσφερόμενο σύστημα θα πρέπει να είναι σε μορφή virtual appliance.	ΝΑΙ		
2.1.4	Υποστήριξη τεχνολογίας Microsoft Hyper-V. Να αναφερθούν και οι υπόλοιποι υποστηριζόμενοι hypervisors.	ΝΑΙ		
2.1.5	Υποστηριζόμενος αποθηκευτικός χώρος.	≥ 1 TB		
2.1.6	Υποστήριξη υψηλής διαθεσιμότητας.	ΝΑΙ		
2.1.7	Υποστήριξη load balancing σε L7	ΝΑΙ		
2.1.8	Η εφαρμογή θα εγκατασταθεί σε υποδομή, η οποία θα παραχωρηθεί από την Αναθέτουσα Αρχή	ΝΑΙ		
2.2	**Επιδόσεις**			
2.2.1	HTTP inspection throughput	≥ 2 Gbps		
2.2.2	Απεριόριστος αριθμός υποστηριζόμενων εφαρμογών	ΝΑΙ		
2.3	**Λειτουργικά Χαρακτηριστικά**			
2.3.1	Λειτουργία reverse proxy	ΝΑΙ		
2.3.2	Διαφανής λειτουργία	ΝΑΙ		
2.3.3	Λειτουργία ως L2 γέφυρα	ΝΑΙ		
2.3.4	Λειτουργία offline (π.χ. packet sniffer πίσω από span θύρα μεταγωγού)	ΝΑΙ		
2.3.5	Υποστήριξη HTTP και HTTPS	ΝΑΙ		
2.3.6	Υποστήριξη HTTP/1.x, HTTP/2	ΝΑΙ		
2.3.7	Υποστήριξη autolearning	ΝΑΙ		
2.3.8	Συνεργασία με εξωτερικό σύστημα sandbox	ΝΑΙ		
2.3.9	Ρυθμίσεις για περιορισμό των false positive (να περιγραφούν αναλυτικά οι δυνατότητες)	ΕΠΙΘΥΜΗΤΟ		
2.3.10	Ομαδοποίηση web server σε πολλαπλά λογικά WAF.	ΝΑΙ		
2.3.11	Υποστήριξη Single Sign On (SSO) στην πρόσβαση στις web υπηρεσίες.	ΝΑΙ		
2.3.12	Συσχέτιση γεγονότων	ΝΑΙ		
2.3.13	Αποσυμφόρηση web server ως προς την λειτουργία πιστοποίησης χρήστη (authentication offload)	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.3.14	Αποσυμφόρηση web server ως προς την λειτουργία της συμπίεσης δεδομένων (compression offload)	ΝΑΙ		
2.3.15	Αποσυμφόρηση web server ως προς την λειτουργία του SSL (SSL offload)	ΝΑΙ		
2.3.16	Υποστήριξη web caching	ΝΑΙ		
2.3.17	Υποστήριξη IPv6	ΝΑΙ		
2.4	**Δυνατότητες Ελέγχου HTTP/HTTPS**			
2.4.1	Περιορισμός χρησιμοποιούμενων πρωτοκόλλων και εκδόσεων πρωτοκόλλων εφαρμογών.	ΝΑΙ		
2.4.2	Αυστηρή συμμόρφωση κατά RFC.	ΝΑΙ		
2.4.3	Επιβεβαίωση URL encoding	ΝΑΙ		
2.4.4	Περιορισμός με βάση το μήκος του περιεχομένου επικεφαλίδας (content length)	ΝΑΙ		
2.4.5	Περιορισμός με βάση το μήκος επικεφαλίδας (header length)	ΝΑΙ		
2.4.6	Έλεγχος HTTP header ως προς μη επιτρεπτούς χαρακτήρες.	ΝΑΙ		
2.4.7	Περιορισμός με βάση το όνομα του cookie	ΝΑΙ		
2.4.8	Δυνατότητα ελέγχου IP reputation	ΝΑΙ		
2.4.9	Δυνατότητα antivirus (ενσωματωμένου)	ΝΑΙ		
2.5	**Δυνατότητες Προστασίας**			
2.5.1	Προστασία σε επίθεση brute force.	ΝΑΙ		
2.5.2	Προστασία cookie μέσω υπογραφής	ΝΑΙ		
2.5.3	Κρυπτογράφηση cookie	ΝΑΙ		
2.5.4	Ανίχνευση αυτοματοποιημένων client	ΝΑΙ		
2.5.5	Προστασία σε DDoS	ΝΑΙ		
2.5.6	Προστασία σε SQL injection	ΝΑΙ		
2.5.7	Προστασία σε cross site scripting	ΝΑΙ		
2.5.8	Προστασία σε session hijacking	ΝΑΙ		
2.5.9	Προστασία σε cross site request forgery	ΝΑΙ		
2.5.10	Προστασία σε web page defacement	ΝΑΙ		
2.5.11	Προστασία έναντι επιθέσεων web με ανάλυση συμπεριφοράς.	ΝΑΙ		
2.5.12	Ενσωματωμένος vulnerability scanner	ΝΑΙ		
2.5.13	Συνεργασία με scanner άλλων κατασκευαστών	ΝΑΙ		
2.5.14	PCI-DSS compliance	ΝΑΙ		
2.6	**Διαχείριση**			

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.6.1	Διαχείριση μέσω γραμμής εντολής (CLI)	ΝΑΙ		
2.6.2	Διαχείριση μέσω ενσωματωμένου γραφικού περιβάλλοντος (GUI)	ΝΑΙ		
2.6.3	Πρόσβαση διαχειριστών μέσω HTTPS και SSH	ΝΑΙ		
2.6.4	Υποστήριξη API για επικοινωνία με εξωτερικές εφαρμογές.	ΝΑΙ		
2.6.5	Συνεργασία με εξωτερικό κεντρικό σύστημα συγκέντρωσης και επεξεργασίας αρχείων καταγραφής (log).	ΝΑΙ		
2.6.6	Γραφικός πίνακας ελέγχου για την απεικόνιση της κατάστασης του συστήματος σε πραγματικό χρόνο.	ΝΑΙ		
2.7	**Υπηρεσίες Υποστήριξης**			
2.7.1	Ο εξοπλισμός θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 διάρκειας 5 ετών.	ΝΑΙ		
2.7.2	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη της λειτουργίας WAF διάρκειας 5 ετών.	ΝΑΙ		

3. Virtual Appliance για την ενιαία διαχείριση των συσκευών NGF, WAF και Web Proxy

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.1	**Επιδόσεις**			
3.1.1	Να αναφερθεί ο κατασκευαστής και το μοντέλο	ΝΑΙ		
3.1.2	Απαιτούμενος αριθμός υποστηριζόμενων συσκευών	≥10		
3.1.3	Υποστήριξη καταγραφής logs ανά ημέρα	≥1 GB		
3.1.4	Υποστήριξη τεχνολογίας Microsoft HyperV. Να αναφερθούν και οι υπόλοιποι υποστηριζόμενοι hypervisors.	ΝΑΙ		
3.1.5	Να αναφερθεί ο αριθμός των υποστηριζόμενων virtual CPU.	ΝΑΙ		
3.1.6	Να αναφερθεί η μέγιστη υποστηριζόμενη μνήμη.	ΝΑΙ		
3.1.7	Η εφαρμογή θα εγκατασταθεί σε υποδομή, η οποία θα παραχωρηθεί από την Αναθέτουσα Αρχή	ΝΑΙ		
3.2	**Λειτουργικά Χαρακτηριστικά**			
3.2.1	Κεντρική διαχείριση συσκευών: Μια ενιαία κονσόλα για διαχείριση όλων των UTM.	ΝΑΙ		
3.2.2	Διαχείριση κεντρικών πολιτικών και αντικειμένων	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
3.2.3	Λεπτομερής παρακολούθηση ιστορικού αναθεωρήσεων και λεπτομερείς δυνατότητες ελέγχου	ΝΑΙ		
3.2.4	Κεντρική διαχείριση VPN	ΝΑΙ		
3.2.5	Υποστήριξη RESTFullAPI για αυτοματοποίηση και ενορχήστρωση	ΝΑΙ		
3.2.6	Κεντρικές αναβαθμίσεις λογισμικού και ενημερώσεις ασφαλείας για τις διαχειριζόμενες συσκευές	ΝΑΙ		
3.2.7	Το λογισμικό διαχείρισης θα πρέπει να έχει εφαρμογή σε γραφικό περιβάλλον και να διαχειρίζεται κεντρικά όλες τις απαιτούμενες λειτουργίες του	ΝΑΙ		
3.2.8	Η λύση θα πρέπει να επιτρέπει κεντρικοποιημένη αναβάθμιση των συστημάτων ασφαλείας σε νεότερες εκδόσεις λογισμικού.	ΝΑΙ		
3.3	**Υπηρεσίες Υποστήριξης**			
3.3.1	Ο εξοπλισμός θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 διάρκειας πέντε (5) ετών .	ΝΑΙ		
3.3.2	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη της απαιτούμενης λειτουργικότητας διάρκειας πέντε (5) ετών	ΝΑΙ		

4. Προμήθεια Virtual appliance για την προστασία των χρηστών κατά την περιήγηση στο διαδίκτυο (Web Proxy)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.1	**Γενικά Χαρακτηριστικά**			
4.1.1	Να αναφερθεί ο κατασκευαστής και το μοντέλο	ΝΑΙ		
4.1.2	Απαιτούμενος αριθμός τεμαχίων	2		
4.1.3	Το προσφερόμενο σύστημα θα πρέπει να είναι σε μορφή virtual appliance.	ΝΑΙ		
4.1.4	Ελάχιστος αριθμός υποστηριζόμενων CPU cores στο εικονικό περιβάλλον	4		
4.1.5	Υποστήριξη τεχνολογίας Microsoft HyperV. Να αναφερθούν και οι υπόλοιποι υποστηριζόμενοι hypervisors.	ΝΑΙ		
4.1.6	Υποστήριξη υψηλής διαθεσιμότητας.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.1.7	Ελάχιστος αριθμός υποστηριζόμενων χρηστών με την παρεχόμενη άδεια	1500		
4.1.8	Μέγιστος αριθμός υποστηριζόμενων χρηστών με μελλοντική αναβάθμιση της άδειας	2000		
4.2	**Λειτουργικά Χαρακτηριστικά**			
4.2.1	Λειτουργία Web Filtering	ΝΑΙ		
4.2.2	Λειτουργία DNS Filtering	ΝΑΙ		
4.2.3	Λειτουργία Video Filtering	ΝΑΙ		
4.2.4	Λειτουργία Application Control	ΝΑΙ		
4.2.5	Λειτουργία IPS	ΕΠΙΘΥΜΗΤΟ		
4.2.6	Λειτουργία AntiVirus	ΝΑΙ		
4.2.7	Λειτουργία Virus Outbreak και Content Disarm	ΝΑΙ		
4.2.8	Λειτουργία Sandboxing στο Cloud	ΝΑΙ		
4.2.9	Υποστήριξη IPv4 και IPv6	ΝΑΙ		
4.2.10	Υποστήριξη Virtual Domains	ΕΠΙΘΥΜΗΤΟ		
4.2.11	Λειτουργεία Client Browser Isolation	ΝΑΙ		
4.2.12	Λειτουργία SSL/SSH Inspection	ΝΑΙ		
4.2.13	Υποστήριξη Web και Video caching	ΝΑΙ		
4.2.14	Υποστήριξη Reverse Web Cache	ΝΑΙ		
4.2.15	Υποστήριξη Traffic Shaping και πολιτικών QoS για την προτεραιοποίηση εφαρμογών	ΝΑΙ		
4.2.16	Υποστήριξη βελτιστοποίησης πρωτοκόλλων HTTP, MAPI, CIFS, FTP και TCP	ΝΑΙ		
4.3	**Διαχείριση**			
4.3.1	Διαχείριση μέσω γραμμής εντολής (CLI)	ΝΑΙ		
4.3.2	Διαχείριση μέσω ενσωματωμένου γραφικού περιβάλλοντος (GUI)	ΝΑΙ		
4.3.3	Πρόσβαση διαχειριστών μέσω HTTPS και SSH	ΝΑΙ		
4.3.4	Υποστήριξη API για επικοινωνία με εξωτερικές εφαρμογές.	ΝΑΙ		
4.3.5	Συνεργασία με εξωτερικό κεντρικό σύστημα συγκέντρωσης και επεξεργασίας αρχείων καταγραφής (log).	ΝΑΙ		
4.3.6	Γραφικός πίνακας ελέγχου για την απεικόνιση της κατάστασης του συστήματος σε πραγματικό χρόνο.	ΝΑΙ		
4.4	**Υπηρεσίες Υποστήριξης**			
4.4.1	Ο εξοπλισμός θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 διάρκειας 5 ετών.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
4.4.2	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη της λειτουργίας Web Proxy διάρκειας 5 ετών.	ΝΑΙ		

5. Λογισμικό δημιουργίας αντιγράφων ασφάλειας

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
5.1	Αριθμός αδειοδοτημένων εικονικών μηχανών (virtual machines) που θα υποστηρίζει το λογισμικό	≥500		
5.2	Δυνατότητα συνεχούς προστασίας με μηδενικές απώλειες δεδομένων για επιλεγμένα υπολογιστικά φορτία, σε όποια χρονική στιγμή και αν συμβεί αστοχία.	ΕΠΙΘΥΜΗΤΟ		
5.3	Υποστήριξη full, incremental εφεδρικών αντιγράφων εικονικών μηχανών χωρίς την χρήση agent software	ΝΑΙ		
5.4	Να υποστηρίζει λειτουργία copy εικονικών μηχανών για την υποστήριξη λειτουργίας μεταφοράς σε άλλο data center ή για archive με δυνατότητα λειτουργίας χειροκίνητα ή σε επιλεγμένο χρόνο.	ΝΑΙ		
5.5	Να υποστηρίζει δυνατότητα δημιουργίας και μεταφοράς φακέλων και αρχείων μεταξύ εξυπηρετητών και κόμβων που έχουν προστεθεί στην υποδομή λήψης αρχείων.	ΝΑΙ		
5.6	Να υποστηρίζει την δυνατότητα επαναφοράς εικονικής μηχανής σε περιβάλλον απομονωμένης λειτουργίας, ώστε να ελέγχεται η εικονική μηχανή για πιθανό malware infection ή προβλήματα στην αναβάθμιση λογισμικού και επιπτώσεις.	ΝΑΙ		
5.7	Να υποστηρίζει δυνατότητα βελτιστοποίησης της μεταφοράς δεδομένων σε απομακρυσμένες υποδομές όπως • Network traffic compression • Multistreaming upload • Global data deduplication • Variable block size deduplication	ΝΑΙ		
5.8	Να υποστηρίζει άμεση ανάκτηση εικονικών μηχανών απευθείας από συμπιεσμένα και “deduplicated” αρχεία αντιγράφων ασφαλείας. Για την επίτευξη καλυτέρου Recovery Time Objective να γίνεται η ανάκτηση απευθείας από το αποθετήριο που έχει αποθηκευτεί το αντίγραφο ασφάλειας.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
5.9	Να υποστηρίζει δυνατότητα ανάκτησης των τοπικών εικονικών μηχανών σε Azure,AWS hyperscale υποδομές καθώς και την δημιουργία εφεδρικών αντιγράφων εικονικών μηχανών που μπορεί να δημιουργηθούν σε αυτούς τους παρόχους.	ΝΑΙ		
5.10	Να υποστηρίζει την επαναφορά εικονικών δίσκων από αντίγραφα ασφαλείας φυσικών ή εικονικών μηχανών και την μετατροπή σε μορφές VMDK, VHD ή VHDX.	ΝΑΙ		
5.11	Να υποστηρίζει την λήψη αντιγράφων ασφαλείας και την επαναφορά των παρακάτω εφαρμογών : • Microsoft Active Directory • Microsoft SQL Server • Oracle • Microsoft Exchange • Microsoft SharePoint • Microsoft OneDrive για επιχειρήσεις • Microsoft Teams	ΝΑΙ		
5.12	Να υποστηρίζεται δημιουργία αντιγράφων ασφαλείας κρυπτογραφημένων VM •Αντιγραφή κρυπτογραφημένων VM •Επαναφορά κρυπτογραφημένων VM •Μετάπτωση κρυπτογραφημένων VM	ΝΑΙ		
5.13	Να παρέχεται η δυνατότητα να επαληθεύεται η ακεραιότητα ενός αρχείου αντιγράφου ασφαλείας χωρίς εξαγωγή δεδομένων από το VM	ΝΑΙ		
5.14	Να παρέχεται η δυνατότητα των ακολουθών μέσων ως αποθετηρίων εικονικών αντιγράφων • Microsoft windows repositories • Linux backup repositories • Dedup storage appliances • Shared folders	ΝΑΙ		
5.15	Να παρέχεται η δυνατότητα ελέγχου υγείας για το πιο πρόσφατο σημείο επαναφοράς στην εφεδρική αλυσίδα για file share backups .	ΝΑΙ		
5.16	Να παρέχεται η δυνατότητα όταν επαναφέρονται δεδομένα από κρυπτογραφημένες κασέτες, να εκτελείται αυτόματα η αποκρυπτογράφηση δεδομένων στο παρασκήνιο	ΕΠΙΘΥΜΗΤΟ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
5.17	Να υποστηρίζεται η δυνατότητα ανάκτησης κοινόχρηστου αρχείου (file-share) SMB σε ζητούμενο χρονικό σημείο με δικαιώματα read-only ώστε οι χρήστες να έχουν πρόσβαση στα προστατευμένα αρχεία	ΝΑΙ		
5.18	Να υποστηρίζεται η δημιουργία αντιγράφων ασφαλείας φυσικών Η/Υ με λειτουργικά συστήματα Windows, Linux.	ΝΑΙ		
5.19	Να υποστηρίζει την δημιουργία αποθετηρίων με δυνατότητα για την επιλεγόμενη από τον οργανισμό χρονική περίοδο τα αρχεία αντιγράφων ασφαλείας να είναι αμετάβλητα. Κατά τη διάρκεια αυτής της περιόδου, τα αρχεία αντιγράφων ασφαλείας που είναι αποθηκευμένα σε αυτό το αποθετήριο δεν μπορούν να τροποποιηθούν ή να διαγραφούν	ΝΑΙ		
5.20	Να προσφερθούν όλες οι απαιτούμενες άδειες χρήσης για τουλάχιστον 500 εικονικές ή φυσικές μηχανές .Οι άδειες χρήσης να είναι τύπου perpetual (μόνιμη άδεια).Η παρεχόμενη υποστήριξη να είναι για τουλάχιστον 4 χρόνια.	ΝΑΙ		
5.21	Ο Ανάδοχος θα κάνει τις κατάλληλες παραμετροποιήσεις στο λογισμικό δημιουργίας αντιγράφων ασφάλειας και αποκατάστασης καταστροφών ώστε να διασυνδεθεί με τα υφιστάμενα συστήματα αποθήκευσης καθώς και με τα συστήματα λήψης αντιγράφων ασφάλειας	ΝΑΙ		
5.22	Η λύση θα πρέπει να σαρώνει το σύστημα αρχείων του guest λειτουργικού συστήματος (guest file system) μέσα σε image-level αντίγραφα ασφαλείας για κακόβουλο λογισμικό, όπως ιούς υπολογιστών ή ransomware, πριν από την επαναφορά στο παραγωγικό περιβάλλον.	ΝΑΙ		
5.23	Η λύση θα πρέπει να παρέχει έναν αυτοματοποιημένο μηχανισμό για τη σάρωση αντιγράφων ασφαλείας εικονικών μηχανών (VM backups) που βρίσκονται σε δίσκους, με σκοπό τον εντοπισμό πιθανής μόλυνσης από ιούς και κακόβουλο λογισμικό, χρησιμοποιώντας την πιο πρόσφατη υπογραφή του λογισμικού προστασίας από ιούς (antivirus software), πριν από την εκτέλεση πλήρους επαναφοράς VM ή δίσκου.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
5.24	Η λύση θα έχει την δυνατότητα να δοκιμάζει τα αντίγραφα ασφαλείας (machine backups) και να επαληθεύει ότι η διαδικασία ανάκτησης (recovery) μπορεί να πραγματοποιηθεί με αξιοπιστία. Αυτό επιτυγχάνεται μέσω της επαλήθευσης οποιουδήποτε restore point μιας συσκευής που διαθέτει αντίγραφο ασφαλείας (backed-up machine). Η λύση θα πρέπει να εκτελεί "live verification", το οποίο περιλαμβάνει: σάρωση των δεδομένων του backup για κακόβουλο λογισμικό (malware), εκκίνηση της συσκευής από το backup σε απομονωμένο περιβάλλον (isolated environment), εκτέλεση δοκιμών στη συσκευή, τερματισμό της (power-off) και δημιουργία αναφοράς με τα αποτελέσματα της επαλήθευσης της ανάκτησης (recovery verification results).	ΕΠΙΘΥΜΗΤΟ		
5.25	Η λύση θα έχει δυνατότητα να σαρώνει τα δεδομένα της συσκευής (machine data) με λογισμικό προστασίας από ιούς (antivirus software) πριν από την επαναφορά της στο παραγωγικό περιβάλλον. Σε περίπτωση που κατά τη σάρωση ανιχνευτεί κακόβουλο λογισμικό (malware), η λύση θα πρέπει να μπορεί είτε να ακυρώνει τη διαδικασία επαναφοράς, είτε να επαναφέρει τη συσκευή ή τους δίσκους της με περιορισμούς, ανάλογα με τις ρυθμίσεις ασφαλούς επαναφοράς (secure restore settings).	ΝΑΙ		
5.26	Η λύση θα έχει δυνατότητα να δοκιμάζει και να επαληθεύει αυτόματα την δυνατότητα ανάκτησης (recoverability) κάθε αντιγράφου ασφαλείας (backup), εκτελώντας την εικονική μηχανή (VM) απευθείας από το αρχείο backup σε απομονωμένο αντίγραφο του παραγωγικού περιβάλλοντος (fenced-off copy of production environment), συμπεριλαμβανομένης της υποστήριξης προσαρμοσμένων σεναρίων δοκιμής εφαρμογών (custom application test scripts).	ΝΑΙ		
5.27	Η λύση πρέπει να δοκιμάζει και να επαληθεύει αυτόματα τη δυνατότητα ανάκτησης (recoverability) κάθε αντιγράφου (replica), πραγματοποιώντας μετάπτωση (failover) σε απομονωμένο αντίγραφο του περιβάλλοντος παραγωγής, με υποστήριξη προσαρμοσμένων σεναρίων δοκιμών εφαρμογών (custom application test scripts).	ΝΑΙ		

6. Λογισμικό Διαχείρισης Προνομιακών Προσβάσεων (Privileged Access Management ή PAM)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.1	Να αναφερθεί το όνομα, η έκδοση και η χρονολογία διάθεσης του προσφερόμενου λογισμικού	ΝΑΙ		
6.2	Απαιτούνται τουλάχιστον είκοσι (20) άδειες χρήσης, που θα καλύπτουν ισάριθμους ονομαστικούς χρήστες/ διαχειριστές	ΝΑΙ		
6.3	Αριθμός των συστημάτων (δικτυακές συσκευές, εικονικές μηχανές) που θα ενταχθούν στο σύστημα κατά την έναρξη παραγωγικής λειτουργίας του.	Δικτυακές Συσκευές: 50 Εικονικές μηχανές: 100		
6.4	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει κλιμακούμενη αδειοδότηση χρηστών, με δυνατότητα διαχείρισης απεριόριστου αριθμού διαπιστευτηρίων	ΝΑΙ		
6.5	Η προτεινόμενη λύση θα πρέπει να παρέχει το σύνολο της λειτουργικότητας της χωρίς να εξαρτάται από τη χρήση λογισμικού άλλου κατασκευαστή.	ΝΑΙ		
6.6	Η προσφερόμενη λύση θα πρέπει να παρέχει το σύνολο της τεκμηρίωσης της και των περιεχομένων της γνωσιακής βάσης στην Αγγλική.	ΝΑΙ		
6.7	Ο κατασκευαστής θα πρέπει να διασφαλίζει παροχή υποστήριξης της λύσης «24x7x365» για κρίσιμα συμβάντα, χωρίς πρόσθετο κόστος	ΝΑΙ		
6.8	Δυνατότητα επιλογής της τοποθεσίας υλοποίησης, είτε στις εγκαταστάσεις του πελάτη, είτε στις εγκαταστάσεις Παρόχων Διαδικτύου (Cloud Providers) όπως Azure, AWS, Google Cloud	ΝΑΙ		
6.9	Δυνατότητα συνδυαστικής υλοποίησης στις εγκαταστάσεις του Πελάτη (on-premises, private cloud) και στις εγκαταστάσεις Διαδικτυακού Παρόχου, παρέχοντας εφεδρεία σε περιβάλλον ανάκαμψης από καταστροφή (DR)	ΝΑΙ		
6.10	Υποστήριξη εξισορρόπησης φορτίου (load-balancing) μεταξύ πολλαπλών υλοποιήσεων/συσκευών, σε περίπτωση αυξημένων απαιτήσεων για επεξεργαστική ισχύ	ΝΑΙ		
6.11	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει δυνατότητα λειτουργίας Υψηλής Διαθεσιμότητας (High Availability) σε τοπολογίες Active/active και Active/Passive	ΝΑΙ		
6.12	Υλοποίηση της λύσης βασιζόμενη σε εικονικές συσκευές που μπορούν να φιλοξενηθούν σε γνωστές πλατφόρμες εικονικοποίησης όπως VMware, Microsoft Hyper-V ή Citrix XenServer	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
6.13	Η προσφερόμενη λύση θα πρέπει να παρέχει κρυπτογράφηση της διαδικτυακής επικοινωνίας με χρήση αλγορίθμου AES-256	ΝΑΙ		
6.14	Η προσφερόμενη λύση θα πρέπει να παρέχει κρυπτογράφηση στοιχείων/δεδομένων με χρήση κωδικοποίηση AES-256 κατά την αποθήκευση	ΝΑΙ		
6.15	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), διακριτά για κάθε χρήστη	ΝΑΙ		
6.16	Τα δεδομένα της λύσης θα πρέπει να διατηρούν τα ίδια επίπεδα ασφάλειας και κρυπτογράφησης κατά την διαδικασία λήψης αντιγράφου ασφαλείας	ΝΑΙ		
6.17	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα αναβάθμισης λογισμικού, χωρίς απαίτηση πλήρους διακοπής της λειτουργίας της στο παραγωγικό περιβάλλον.	ΕΠΙΘΥΜΗΤΟ		
6.18	Η προσφερόμενη λύση θα πρέπει να παρέχει τις αναβαθμίσεις ασφάλειας του λογισμικού: α) αυτοματοποιημένα, και β) κατ' επιλογή	ΝΑΙ		
6.19	Η προσφερόμενη λύση θα πρέπει να παρέχει κεντρικό και ενιαίο περιβάλλον ελέγχου και διαχείρισης, των λογαριασμών και κωδικών πρόσβασης.	ΝΑΙ		
6.20	Δυνατότητα αυτόματης αναζήτησης των συσκευών/συστημάτων, λογαριασμών και των στοιχείων πρόσβασης τους (devices, accounts & credentials), προς ένταξη τους στο περιβάλλον κεντρικού ελέγχου και διαχείρισης	ΝΑΙ		
6.21	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει κατ' ελάχιστο, τη διασύνδεση και διαχείριση προνομιακών λογαριασμών και προσβάσεων για τα ακόλουθα συστήματα: • Active Directory, LDAP directories • Windows (versions Desktop 7, 10, 11, Server 2012/2016/2019/2022) • Unix and Linux (AIX, Solaris, Red Hat, SUSE, Debian, Fedora, Ubuntu) • DB2, Oracle, SQL, MySQL, MongoDB, PostgreSQL, SAP HANA databases • Network Devices of well-known vendors (CheckPoint, Palo Alto, Aruba, Extreme, FortiGate, Juniper, HP, Huawei, IBM, Cisco, Citrix, Dell, F5, Sophos, Watchguard, etc.) • Virtualization Environments (Hyper-V, VMware, XenServer) and major Cloud platforms (Azure, AWS, GCP)	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Web applications, προσβάσιμες μέσω γνωστών προγραμμάτων περιήγησης (Microsoft Edge, Chrome, Mozilla Firefox etc.)			
6.22	Η πρόσβαση στην προσφερόμενη λύση θα πρέπει να επιτυγχάνεται με τη χρήση των υφιστάμενων διαπιστευτηρίων των χρηστών και χωρίς την απαίτηση εγκατάστασης λογισμικού (agents) στα διαχειριζόμενα συστήματα	ΝΑΙ		
6.23	Δυνατότητα διασύνδεσης με καταλόγους LDAP και AD, με σκοπό των έλεγχο πρόσβασης, σύμφωνα με μηχανισμό RBAC (Role Based Access Control)	ΝΑΙ		
6.24	Αυτοματοποιημένες εναλλαγές (rotation) των αποθηκευμένων κωδικών πρόσβασης, σε τακτά χρονικά διαστήματα, σύμφωνα με προκαθορισμένες πολιτικές	ΝΑΙ		
6.25	Δυνατότητα εφαρμογής διακριτών, αυστηρών πολιτικών (password policy) για τη διαμόρφωση των κωδικών ασφάλειας/πρόσβασης με πολλαπλά κριτήρια όπως ελάχιστο μήκος κωδικών, πολυπλοκότητα, συχνότητα εναλλαγής	ΝΑΙ		
6.26	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει την παροχή ελεγχόμενης πρόσβασης μέσω εγκριτικής διαδικασίας (απλή ή πολλαπλή έγκριση), με δυνατότητα χρονικού περιορισμού. Να αναφερθεί αναλυτικά	ΝΑΙ		
6.27	Δυνατότητα διαμόρφωσης πολιτικών ελέγχου πρόσβασης με βάσει μοντέλο Just-in-Time (JIT), ώστε πέραν των άλλων να λαμβάνονται υπόψη συνθήκες ή/και παράμετροι όπως ημέρα/ώρα, τοποθεσία/ διεύθυνση IP	ΝΑΙ		
6.28	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει τη δημιουργία συνεδρίας αυξημένων δικαιωμάτων για τη σύνδεση των διαχειριστών σε συστήματα Unix, Linux και Δικτυακές Συσκευές μέσω πρωτοκόλλου SSH	ΝΑΙ		
6.29	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει τη δημιουργία συνεδρίας αυξημένων δικαιωμάτων για τη σύνδεση των διαχειριστών σε συστήματα Windows μέσω πρωτοκόλλου RDP	ΝΑΙ		
6.30	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα τερματισμού ή αποκλεισμού μιας συνεδρίας (session) η οποία έχει υλοποιηθεί με χρήση αυξημένων δικαιωμάτων, είτε λόγω αδράνειας είτε μετά από αίτημα του διαχειριστή	ΝΑΙ		
6.31	Η προσφερόμενη λύση θα πρέπει να παρέχει τη δυνατότητα άμεσου αποκλεισμού της πρόσβασης ενός χρήστη στην πλατφόρμα διαχείρισης και τα διαχειριζόμενα συστήματα, μέσω μοναδικής	ΕΠΙΘΥΜΗΤΟ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	εντολής αναίρεσης του συνόλου των δικαιωμάτων του			
6.32	Πλήρης και διαρκής καταγραφή των ενεργειών/λειτουργιών που αφορούν τις αυτοματοποιημένες αλλαγές των κωδικών πρόσβασης που χρησιμοποιούν οι μηχανές αυτοματοποίησης ή/και τους Διαχειριστές, ώστε να διασφαλίζεται η ανιχνευσιμότητα τους και η κανονιστική συμμόρφωση	ΝΑΙ		
6.33	Προηγμένη ανάλυση καταγεγραμμένων ενεργειών/λειτουργιών, με σκοπό την ανίχνευση πιθανών απειλών, που προκύπτουν κατά τη χρήση της πλατφόρμας	ΝΑΙ		
6.34	Δυνατότητα διασύνδεσης με λογισμικό άλλων κατασκευαστών, μέσω Application Programming Interface (API), με σκοπό τη λειτουργική ενοποίηση και περαιτέρω αξιοποίηση των χαρακτηριστικών και δυνατοτήτων της λύσης	ΝΑΙ		

7. Προμήθεια Λογισμικού Ανάλυσης και Παρακολούθησης Δικτύου

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
7.1	**Γενικά Χαρακτηριστικά**			
7.1.1	Να αναφερθεί ο κατασκευαστής και το μοντέλο	ΝΑΙ		
7.1.2	Απαιτούμενος αριθμός αισθητήρων (sensors)	≥15000		
7.1.3	Το προσφερόμενο σύστημα θα πρέπει να διαθέτει διαχειριστικό εργαλείο που να μπορεί να υλοποιηθεί on-premise	ΝΑΙ		
7.1.4	Η εφαρμογή θα εγκατασταθεί σε υποδομή, η οποία θα παραχωρηθεί από την Αναθέτουσα Αρχή	ΝΑΙ		
7.2	**Λειτουργικά Χαρακτηριστικά**			
7.2.1	Υποστήριξη παρακολούθησης Hardware, Software, Virtual Environments και εφαρμογών	ΝΑΙ		
7.2.2	Υποστήριξη παρακολούθησης Windows, Linux και MacOS χωρίς τη χρήση agent	ΝΑΙ		
7.2.3	Υποστήριξη κοινών πρωτοκόλλων (SNMP, WMI, ICMP, HTTP, MQTT, SOAP, SSH, FTP, SMTP, POP3, DICOM, HL7)	ΝΑΙ		
7.2.4	Υποστήριξη NetFlow v5/v9, sFlow, jFlow, IPFIX και packet sniffing	ΝΑΙ		
7.2.5	Υποστήριξη Restful API και Custom Sensors για παρακολούθηση	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
7.2.6	Υποστήριξη Auto-discovery & Smart Setup για εύκολη παραμετροποίηση	ΝΑΙ		
7.2.7	Ύπαρξη Preconfigured templates για κοινές συσκευές και εφαρμογές	ΕΠΙΘΥΜΗΤΟ		
7.2.8	Υποστήριξη παρακολούθησης πολλαπλών τοποθεσιών με μία κεντρική εγκατάσταση	ΝΑΙ		
7.2.9	Ενσωματωμένη βάση δεδομένων χωρίς να απαιτείται χρήση εξωτερικής	ΝΑΙ		
7.2.10	Ενσωματωμένος mail και web server	ΝΑΙ		
7.2.11	Ύπαρξη mobile applications (Android και iOS)	ΕΠΙΘΥΜΗΤΟ		
7.3	**Διαχείριση**			
7.3.1	Γραφικό περιβάλλον (Dashboard) για την απεικόνιση της κατάστασης του συστήματος σε πραγματικό χρόνο.	ΝΑΙ		
7.3.2	Δυνατότητα διαχείρισης μέσω εφαρμογής desktop Windows/MacOS	ΝΑΙ		
7.3.3	Δυνατότητα διαχείρισης μέσω browser	ΝΑΙ		
7.3.4	Δυνατότητα διαχείρισης μέσω εφαρμογής κινητού Android/iOS	ΝΑΙ		
7.3.5	Δυνατότητα υλοποίησης πολλαπλών monitoring servers και κεντρικής διαχείρισής τους	ΝΑΙ		
7.3.6	Δυνατότητα εξαγωγής reports σε HTML, PDF	ΝΑΙ		
7.3.7	Δυνατότητα αποστολής ειδοποιήσεων μέσω email, SMS, Slack, Microsoft Teams, push notifications, HTTP request, syslog)	ΝΑΙ		
7.3.8	Δυνατότητα συνεργασίας και αποστολής logs σε εξωτερικό κεντρικό σύστημα συγκέντρωσης και επεξεργασίας αρχείων καταγραφής (siem).	ΝΑΙ		
7.4	**Υπηρεσίες Υποστήριξης**			
7.4.1	Το λογισμικό θα πρέπει να προσφερθεί με υπηρεσίες υποστήριξης 24x7 διάρκειας 5 ετών.	ΝΑΙ		
7.4.2	Θα πρέπει να προσφερθούν όλες οι άδειες χρήσης που απαιτούνται για την υποστήριξη της λειτουργίας του Network Monitoring Tool διάρκειας 5 ετών.	ΝΑΙ		

8. Λογισμικό Asset Management

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
8.1	Να αναφερθεί το όνομα, η έκδοση και η χρονολογία διάθεσης του προσφερόμενου λογισμικού	ΝΑΙ		
8.2	Συνεχής ορατότητα σε endpoint καταστάσεις, εφαρμογές, ευπάθειες	ΝΑΙ		
8.3	Δυνατότητες διαχείρισης απομακρυσμένων συσκευών (remote remediation, remote access)	ΝΑΙ		
8.4	Αυτόματη παρακολούθηση υγείας εφαρμογών & επανόρθωση κρίσιμων εφαρμογών	ΝΑΙ		
8.5	Διαχείριση patches για OS & third-party εφαρμογές	ΝΑΙ		
8.6	Αποκατάσταση (recovery) των endpoints σε πιστή κατάσταση όταν υπάρξουν σοβαρά προβλήματα (OS corrupt, malware κ.ά.)	ΝΑΙ		
8.7	Εκτέλεση προκαθορισμένων σεναρίων αποκατάστασης / συντήρησης, ενσωμάτωση με SIEM / SOAR	ΝΑΙ		
8.8	Έλεγχος πρόσβασης στη διαχείριση recovery / playbooks βάσει ρόλων	ΝΑΙ		
8.9	Προτεραιοποίηση patches / δράσεων βάση κινδύνου	ΕΠΙΘΥΜΗΤΟ		
8.10	Εκθέσεις συμμόρφωσης σχετικές με patches / ευπάθειες / κατάσταση endpoints	ΕΠΙΘΥΜΗΤΟ		
8.11	Ασφάλεια τερματικών συσκευών ενσωματωμένη στο υλικολογισμικό (firmware)	ΝΑΙ		

9. Πλατφόρμα περιορισμού Ransomware

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
9.1	**Χαρακτηριστικά Πλατφόρμας**			
	Η πλατφόρμα να διαθέτει τις παρακάτω λειτουργίες:			
9.1.1	**Πίνακας Ελέγχου Live, προβολή και παρακολούθηση** • Ζωντανό και Καταγεγραμμένο Ημερολόγιο • Ανάλυση επιπέδου ειδοποιήσεων Χρήστη και Διακομιστή • Ζωντανή Δραστηριότητα και ως Ραντάρ • Ιστορικό Δραστηριότητας • Μηνύματα κατάστασης και ειδοποιήσεις	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Αναζήτηση σε ημερολόγια και συμβάντα • Γενική λειτουργία αναζήτησης			
9.1.2	**Ζώνες Παρακολούθησης** • Παρακολούθηση κοινόχρηστων αρχείων SMB/CIFS των Windows • Παρακολούθηση κοινόχρηστων αρχείων που υποστηρίζουν SMB/CIFS, όπως πλατφόρμες αποθήκευσης Isilon και NetApp που συμμορφώνονται με τις προδιαγραφές SMB σύμφωνα με τη Microsoft. • Ρύθμιση κατάστασης κοινόχρηστων αρχείων, διακόπτη ασφαλείας και άλλων παραμέτρων • Παρακολούθηση κρίσιμης υποδομής πληροφορικής και ρύθμιση διακομιστών • Παρακολούθηση Domain Controllers, Διακομιστών Web, Εφαρμογών, Βάσεων Δεδομένων και Windows Servers που χρησιμοποιούνται στο κέντρο δεδομένων • Εξαγωγή/εισαγωγή λιστών σε μορφή CSV • Προσθήκη ή αφαίρεση εγγραφών μέσω API • Σύνδεση DFS	ΝΑΙ		
9.1.3	**Σύνδεσμος Office 365** • Ανίχνευση κρυπτογράφησης όταν συγχρονίζονται ή ανεβαίνουν έγγραφα του OneDrive, του SharePoint και του Teams • Αυτόματη προσθήκη νέων χρηστών και τοποθεσιών για παρακολούθηση • Πιστοποίηση μέσω Client/Secret	ΝΑΙ		
9.1.4	**Σύνδεσμος Google** • Ανίχνευση κρυπτογράφησης όταν συγχρονίζονται ή ανεβαίνουν έγγραφα Google • Πιστοποίηση μέσω Client/Secret	ΕΠΙΘΥΜΗΤΟ		
9.1.5	**Γνωστό Κακόβουλο Λογισμικό Ransomware** • Αυτόματη ενημέρωση γνωστών κακόβουλων υπογραφών Ransomware κάθε 15 λεπτά • Γνωστές κακόβουλες Επεκτάσεις, Ευρετικά Αρχείων, Τεχνουργήματα	ΝΑΙ		
9.1.6	**Δημιουργία Λευκής Λίστας Βασικής Γραμμής με Χρήση Μηχανικής Μάθησης** • Αυτόματη προσθήκη στη λευκή λίστα γνωστής αξιόπιστης κίνησης SMB	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Λίστα επεκτάσεων, ευρετικών αρχείων, διπλών επεκτάσεων			
9.1.7	**Πίνακας Επισκόπησης Ειδοποιήσεων** • Λίστα όλων των ειδοποιήσεων • Κατάσταση όλων των ειδοποιήσεων • Χειροκίνητη και ομαδική προσθήκη συμβάντων στη λευκή λίστα • Λίστα εκτελεσμένων Scripts • Λίστα Συμβάντων και Αρχείων • Αντίστροφη εκτέλεση Scripts/Απομόνωση • Περίληψη Συμβάντων • Εξαγωγή σε μορφή CSV	ΝΑΙ		
9.1.8	**Ανίχνευση Κρυπτογράφησης** • Χρήση 10 αισθητήρων για την άμεση ανίχνευση κρυπτογράφησης. • Ενσωμάτωση 14 αισθητήρων που συνδυάζουν δεδομένα για ακριβέστερη ανίχνευση. • 4 Προγραμματιζόμενοι Αισθητήρες που βασίζονται σε scripts για εξειδικευμένη ανίχνευση. • Διακριτές Ρυθμίσεις Αισθητήρων για το Cloud Διαμόρφωση ξεχωριστών παραμέτρων για αισθητήρες που παρακολουθούν δραστηριότητες στο cloud. • Προσαρμογή Ορίων και Όλων των Παραμέτρων Αισθητήρων	ΝΑΙ		
9.1.9	**Ειδοποιήσεις** • Ειδοποιήσεις μέσω SMTP / e-mail, μεμονωμένες ή ομαδικές, Microsoft Graph • Προσαρμογή συχνότητας και ρυθμίσεων ειδοποιήσεων • Ρύθμιση ενσωμάτωσης με SIEM και Ειδοποιήσεις • Αυτόματες ειδοποιήσεις 24/7	ΝΑΙ		
9.1.10	**Αντιμετώπιση** • Πλήρες προσχέδιο πλάνου απόκρισης (ενημερώνεται κατά την υλοποίηση) • Λειτουργικότητα λίστας περιουσιακών στοιχείων για hosts και συσκευές, αν απαιτείται • Αρχιτεκτονική Plugin Scripts χρησιμοποιώντας PowerShell	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Έλεγχος και ρύθμιση παραμέτρων και λεπτομερειών όλων των scripts • Δημιουργία πολυεπίπεδων αποκρίσεων • Αυτόματη Αντιμετώπιση και Πολυεπίπεδη Απομόνωση 24/7			
9.1.11	**Ενσωμάτωση** • Ενσωμάτωση με οποιοδήποτε σύστημα που υποστηρίζει API • Έτοιμη ενσωμάτωση για περισσότερα από 60 διαφορετικά συστήματα AV/EDR/XDR/SIEM • Υποστήριξη ενσωμάτωσης για οποιοδήποτε VPN, NAC, Helpdesk, AD, Cloud κ.λπ. • Αρχιτεκτονική Plugin Scripts για ενσωμάτωση χρησιμοποιώντας PowerShell	ΝΑΙ		
9.1.12	**Ανάκτηση** • Δημιουργία αναφοράς ανάκτησης/λίστας αρχείων και καταλόγων μετά τον τερματισμό μιας επίθεσης • Εξαγωγή λίστας σε μορφή CSV • Δημιουργία script για ενσωμάτωση με λύση Backup • Δημιουργία αναφορών GDPR σε μορφή PDF	ΝΑΙ		
9.1.13	**Αναφορά** • Δημιουργία στατιστικών και αναφορών κατάστασης για την παρακολούθηση	ΕΠΙΘΥΜΗΤΟ		
9.1.14	**Ασφάλεια** • Πιστοποιητικά/HTTPS/PFX • Ειδοποιήσεις για τη λήξη πιστοποιητικών • Υποστήριξη TLS 1.2 και 1.3 • Χρήση διαπιστευτηρίων χρηστών από το Active Directory (AD) • Επίπεδα ασφαλείας: Master, Admin, View • Σύνδεση με Πολυπαραγοντικό Έλεγχο Ταυτότητας (MFA)	ΝΑΙ		
9.1.15	**Σύστημα** • Υποστήριξη Διακομιστή SYSLOG για συλλογή και καταγραφή δεδομένων συστήματος. • Λειτουργία Αυτόματης Ενημέρωσης. • Υποστήριξη Εξωτερικού MS SQL Server.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Αυτόματη Δημιουργία Τεκμηρίωσης ρυθμίσεων Συστήματος • Ρύθμιση Master Slave Υποστήριξη για ρυθμίσεις κύριου και δευτερεύοντος διακομιστή για αυξημένη αξιοπιστία και απόδοση.			
9.1.16	**Υπηρεσίες** • Παροχή ενημερώσεων για τη συνδρομή χωρίς επιπλέον κόστος για 5 χρόνια • Παροχή υποστήριξης για τη διαχείριση και χρήση της συνδρομής, χωρίς επιπλέον κόστος για 5 χρόνια	ΝΑΙ		

Β1. Υπηρεσίες

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	Απαίτηση	Απάντηση	Παραπομπή
Β1.1	**Υπηρεσίες Υποστήριξης**			
1.1.1	Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει οργανωμένο helpdesk με ON-CALL μηχανικό για την εξυπηρέτηση των αιτημάτων του παρόντος έργου, για όλο το διάστημα εγγύησης καλής λειτουργίας και υποστήριξης και κατά τις εργάσιμες ημέρες και ώρες.	ΝΑΙ		
1.1.2	Στο χρονικό διάστημα κατά το οποίο ο υπό προμήθεια εξοπλισμός βρίσκεται σε καθεστώς εγγύησης, σε κάθε περίπτωση βλάβης, τεχνικός του Φορέα θα ενημερώνει εγγράφως με e-mail το γραφείο τεχνικής υποστήριξης (helpdesk) του Αναδόχου.	ΝΑΙ		
1.1.3	Κατά την διάρκεια της περιόδου εγγύησης, ο υποψήφιος Ανάδοχος δεσμεύεται για την αποκατάσταση οποιασδήποτε βλάβης εξοπλισμού το αργότερο εντός δύο (2) εργασίμων ημερών. Η προθεσμία για την αποκατάσταση της βλάβης μετράται από την επομένη ημέρα της έγγραφης ειδοποίησης από την Αναθέτουσα Αρχή προς τον ανάδοχο.	ΝΑΙ		
1.1.4	Ως αποκατάσταση βλάβης νοείται η πλήρης λειτουργική επανένταξη του επισκευασθέντος η/και αντικατασταθέντος εξοπλισμού στο datacenter της Αναθέτουσας Αρχής και η πλήρης αποκατάσταση της λειτουργίας των υπηρεσιών οι οποίες είχαν διακοπεί ή παρακωλυθεί λόγω της βλάβης. Για την ικανοποίηση της ως άνω συμβατικής δέσμευσης, ο Ανάδοχος μπορεί να χρησιμοποιήσει οποιοδήποτε μέσον θεωρήσει πρόσφορο και το οποίο δεν θα αντίκειται σε όρους της σύμβασης.	ΝΑΙ		
Β1.2	**Υπηρεσίες Ανίχνευσης και Αποτίμησης Ευπαθειών**			
1.2.1	Να προσδιορισθεί ο ζητούμενος αριθμός ελεγχόμενων συσκευών και συστημάτων.	500		
1.2.2	Θα πρέπει να ανιχνεύονται ευπάθειες και αδυναμίες σε επίπεδο λειτουργικών συστημάτων, δικτυακών συσκευών, τερματικών συσκευών και Web Εφαρμογών.	ΝΑΙ		
1.2.3	Θα πρέπει να παρέχονται διαφορετικές πολιτικές ελέγχου ανάλογα με το είδος των συστημάτων, το επιθυμητό βάθος του ελέγχου.	ΝΑΙ		
1.2.4	Να υποστηρίζεται η εκτέλεση των ελέγχων ασφάλειας στα συστήματα της υποδομής **χωρίς να απαιτείται η εγκατάσταση ειδικού λογισμικού (agent) σε αυτά (agent-less).**	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	Απαίτηση	Απάντηση	Παραπομπή
1.2.5	Παραγωγή διαφορετικών τύπων αναφορών για διαφορετικού τύπου παραλήπτες όπως λεπτομερείς τεχνικές αναφορές αποκατάστασης αδυναμιών (technical remediation reports) προς τους διαχειριστές της υποδομής, καθώς και συνοπτικές αναφορές υψηλού επιπέδου προς τη διοίκηση (high level executive reports).	ΝΑΙ		
1.2.6	Προτάσεις για περιορισμό αδυναμιών.	ΝΑΙ		

Β2. Υπηρεσίες Παρακολούθησης και Διαχείρισης της Ασφάλειας του Δικτύου Δεδομένων 24 x 7 για χρονικό διάστημα 3 ετών από Security Operation Center

με εγκατεστημένα τα ακόλουθα λογισμικά:

- Security Information Event Management (S.I.E.M.), **και** Threat Intelligence με χρήση τεχνολογίας «κυβερνοπαγίδων».
- Security, Orchestration, Automation, And Response (S.O.A.R.),

1. Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας (Security Information Event Management)

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1	SIEM			
1.1.1	Η προτεινόμενη τεχνολογική λύση SIEM πρέπει να έχει αναγνωριστεί και να έχει συμπεριληφθεί τουλάχιστον μία (1) φορά σε τεχνολογική αξιολόγηση (από Gartner ή Forrester) κατά τα τελευταία τρία (3) έτη. Ο Ανάδοχος υποχρεούται να υποβάλει τεκμηριωμένα αποδεικτικά στοιχεία προς επιβεβαίωση των ανωτέρω.	ΝΑΙ		
1.1.2	Η πλατφόρμα SIEM πρέπει να παρέχεται από προμηθευτή με έδρα, ιδιοκτησία και λειτουργία εντός της Ευρωπαϊκής Ένωσης, με την τεχνολογία, την επεξεργασία δεδομένων, την υποστήριξη και τις λειτουργίες παροχής υπηρεσιών να πραγματοποιούνται υπό τη δικαιοδοσία της ΕΕ και χωρίς εξάρτηση από οντότητες εκτός ΕΕ, σύμφωνα με τις κατευθυντήριες γραμμές του Πλαισίου Κυριαρχίας στο Υπολογιστικό Νέφος (Cloud Sovereignty Framework) της Ευρωπαϊκής Επιτροπής.	ΕΠΙΘΥΜΗΤΟ		
1.1.3	Η προτεινόμενη τεχνολογική λύση SIEM πρέπει να συντηρείται ενεργά, να διαθέτει σαφώς καθορισμένο product roadmap και versioning strategy, διασφαλίζοντας ότι δεν θα περιέλθει σε κατάσταση end-of-life καθ' όλη τη διάρκεια ισχύος της σύμβασης.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1.4	Ο Ανάδοχος πρέπει να έχει την πλήρη ευθύνη διαχείρισης, συντήρησης και ενημέρωσης της πλατφόρμας SIEM που παρέχεται στο πλαίσιο της υπηρεσίας. Αυτές περιλαμβάνουν, κατ' ελάχιστον, την εφαρμογή των security patches, firmware upgrades, software version updates, vulnerability fixes, καθώς και κάθε απαιτούμενη βελτίωση, ώστε να διασφαλίζεται ότι η πλατφόρμα παραμένει ασφαλής, πλήρως λειτουργική και σύμφωνη με τα ισχύοντα διεθνή πρότυπα και τις βέλτιστες πρακτικές.	ΝΑΙ		
1.1.5	Ο Ανάδοχος απαιτείται να περιγράψει τεκμηριωμένα τον τρόπο με τον οποίο εφαρμόζονται όλες οι ενημερώσεις και patches έγκαιρα και χωρίς διακοπή της παρεχόμενης υπηρεσίας. Ο Ανάδοχος υποχρεούται να παρέχει πλήρη τεκμηρίωση σχετικά με το πρόγραμμα ενημερώσεων, τις διαδικασίες του change management και διαδικασίες rollback σε περίπτωση αποτυχίας ενημέρωσης.	ΝΑΙ		
1.1.6	Η λύση SIEM, θα πρέπει να υποστηρίζει ρυθμό συλλογής των δεδομένων καταγραφής από τα υπό παρακολούθηση συστήματα της Αναθέτουσας Αρχής κατ' ελάχιστο : • 6.000 Events Per Second (EPS), στις περιπτώσεις όπου η αδειοδότηση της προσφερόμενης λύσης βασίζεται σε Events Per Second, **ή** • 200 GB ανά ημέρα, στις περιπτώσεις όπου η αδειοδότηση της προσφερόμενης λύσης βασίζεται σε όγκο δεδομένων (GB/day).	ΝΑΙ		
1.1.7	Οι διαδικασίες μεταφοράς Logs και Telemetry οφείλουν να είναι ελεγχόμενες, να παρακολουθούνται συνεχώς και να υπόκεινται σε πλήρη καταγραφή audit trail.	ΝΑΙ		
1.1.8	Για τη διαδικασία συλλογής Logs, η προτεινόμενη λύση πρέπει να υποστηρίζει την εγκατάσταση είτε physical είτε virtual collector appliances στις εγκαταστάσεις της Αναθέτουσας Αρχής. Ο on-site collector πρέπει να εκτελεί τοπικά λειτουργίες, συμπεριλαμβανομένων κατ' ελάχιστον των πιο κάτω: • Log collection • Analysis • Normalization • Archiving και • Correlation	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	Πριν από τη αποστολή των δεδομένων στο κεντρικό SOC περιβάλλον.			
1.1.9	Η συσκευή collector πρέπει να υποστηρίζει εγκατάσταση σε on-premises, private ή public cloud περιβάλλοντα για να παρέχει απρόσκοπτη ενσωμάτωση παρακολούθησης ασφαλείας και διαχείρισης συμβάντων σε διαφορετικά ψηφιακά οικοσυστήματα.	ΝΑΙ		
1.1.10	Οι collectors απαιτείται να υποστηρίζουν συνεχή συλλογή raw logs και events από το σύνολο των επιτηρούμενων συστημάτων.	ΝΑΙ		
1.1.11	Η προτεινόμενη λύση απαιτείται να υποστηρίζει δυνατότητες granular **data masking**, επιτρέποντας στην Αναθέτουσα Αρχή να ορίζει συγκεκριμένα data fields προς απόκρυψη. Όλες οι διαδικασίες data masking οφείλουν να εκτελούνται τοπικά σε επίπεδο collector πριν από οποιαδήποτε μετάδοση δεδομένων στα κέντρα δεδομένων του Αναδόχου. Ο Ανάδοχος υποχρεούται να διασφαλίζει ότι κανένα από τα ευαίσθητα δεδομένα που έχει επιλεγεί για masking δεν εξέρχεται από το περιβάλλον του πελάτη ούτε μεταδίδεται προς το περιβάλλον του SOC σε unmasked μορφή.	ΕΠΙΘΥΜΗΤΟ		
1.1.12	Η προτεινόμενη λύση απαιτείται να υποστηρίζει την αρχειοθέτηση (archive) των raw log data στις εγκαταστάσεις του πελάτη. Τα αρχειοθετημένα δεδομένα πρέπει να υπογράφονται ψηφιακά, να συμπιέζονται και να κρυπτογραφούνται.	ΕΠΙΘΥΜΗΤΟ		
1.1.13	Οποιαδήποτε αποθηκευμένα credentials, κλειδιά κρυπτογράφησης ή κωδικοί πρόσβασης πρέπει να προστατεύονται χρησιμοποιώντας τεχνικές secure hashing.	ΝΑΙ		
1.1.14	Η διαδικασία log normalization πρέπει να εκτελείται αποκλειστικά σε αντίγραφα των raw log data.	ΝΑΙ		
1.1.15	Το μοντέλο κατανάλωσης πρέπει να μην επιβάλλει περιορισμούς στον αριθμό των log sources που δύνανται να ενταχθούν στην προτεινόμενη λύση.	ΕΠΙΘΥΜΗΤΟ		
1.1.16	Η προτεινόμενη λύση πρέπει να υποστηρίζει multi-tenant περιβάλλον με λογικό και ασφαλή διαχωρισμό μεταξύ των tenants.	ΝΑΙ		
1.1.17	Η προτεινόμενη λύση πρέπει να υποστηρίζει την συλλογή των logs με κατ' ελάχιστον τις ακόλουθες μεθόδους: • Syslog forwarding • APIs	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Cloud storage buckets • Local event storage • Log Analytics Storages			
1.1.18	Ο Ανάδοχος πρέπει να υποβάλει αναλυτική περιγραφή του προτεινόμενου μοντέλου παράδοσης και της αρχιτεκτονικής της λύσης. Απαιτείται η λεπτομερής αποτύπωση όλων των στοιχείων που απαιτείται να εγκατασταθούν στις εγκαταστάσεις της Αναθέτουσας Αρχής, καθώς και της μεθοδολογίας μεταφοράς των Logs προς το περιβάλλον του SOC.	ΝΑΙ		
1.1.19	Η προτεινόμενη λύση πρέπει να μπορεί να προσφέρει διαφορετικές μεθόδους για συσχέτιση των logs όπως: • Rule-based • Statistics-based • Historical based • Human-based	ΝΑΙ		
1.1.20	Η προτεινόμενη λύση πρέπει να υποστηρίζει τουλάχιστον τις παρακάτω μεθόδους MFA (Multi Factor Authentication) για σύνδεση στην πλατφόρμα SIEM. • SMS • Push notifications • Email	ΝΑΙ		
1.1.21	Η προτεινόμενη λύση πρέπει να υποστηρίζει τη ρύθμιση εξουσιοδοτημένης κύριας και δευτερεύουσας login τοποθεσίας. Πρόσβαση που προέρχεται εκτός των καθορισμένων αυτών τοποθεσιών πρέπει να δημιουργεί security alert εντός του συστήματος και να απαιτεί την εκτέλεση επιπρόσθετων authentication steps.	ΕΠΙΘΥΜΗΤΟ		
1.1.22	Η λύση SIEM πρέπει να υποστηρίζει προβολή των log data σε πραγματικό χρόνο (Live Data Search) για normalized logs, με δυνατότητα διατήρησης των δεδομένων αυτών μέσω της πλατφόρμας, καθώς και δυνατότητα συσχέτισής τους με αναγνωρισμένα Indicators of Attack (IoCs). Η λύση πρέπει να παρέχει δυνατότητες αναζήτησης των δεδομένων για χρονικό διάστημα τεσσάρων (4) εβδομάδων.	ΝΑΙ		
1.1.23	Η προτεινόμενη λύση πρέπει να υποστηρίζει log retention για χρονικό διάστημα έξι (6) μηνών. Ο Ανάδοχος υποχρεούται να περιλαμβάνει στο πλαίσιο της προσφερόμενης λύσης οποιαδήποτε σχετική άδεια	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	χρήσης (license) απαιτείται για την κάλυψη της ανωτέρω απαίτησης.			
1.1.24	Η προτεινόμενη λύση πρέπει να ευθυγραμμίζεται με το πλαίσιο του MITRE ATT&CK και να υποστηρίζει την αυτόματη αντιστοίχιση των incidents με τις αντίστοιχες τακτικές και τεχνικές. Οι διαδικασίες εντόπισης των απειλών, διερεύνησης, ιεράρχησης ενεργειών απόκρισης, εντοπισμού κενών ασφάλειας και αναφορών οφείλουν να βασίζονται στη μεθοδολογία MITRE ATT&CK.	ΝΑΙ		
1.1.25	Η προτεινόμενη λύση πρέπει να παρέχει τη δυνατότητα στους χρήστες της πλατφόρμας SIEM να έχουν πρόσβαση στα correlation rules που αντιστοιχίζονται σε κάθε MITRE ATT&CK τακτική/τεχνική που έχει υλοποιηθεί εντός του περιβάλλοντος. Απαιτείται πλήρης ευθυγράμμιση με το πλαίσιο MITRE ATT&CK, με δυνατότητα αυτόματης αντιστοίχισης correlation rules σε τακτική/τεχνική και μεθόδους εντοπισμού.	ΝΑΙ		
1.1.26	Η προτεινόμενη λύση πρέπει να υποστηρίζει **Sigma Rules** και να παρέχει δυνατότητες στους χρήστες να εισάγουν τα δικά τους προσαρμοσμένα Sigma rules.	ΝΑΙ		
1.1.27	Η προτεινόμενη λύση πρέπει να μπορεί να υποστηρίζει custom parsers προκειμένου να μπορεί να συλλέγει και να αναλύει logs από μη υποστηριζόμενες πηγές.	ΝΑΙ		
1.1.28	Ο Ανάδοχος απαιτείται να περιγράψει τεκμηριωμένα τη διαδικασία ενσωμάτωσης οποιωνδήποτε μη υποστηριζόμενων log sources στην πλατφόρμα.	ΝΑΙ		
1.1.29	Η προτεινόμενη λύση πρέπει να παρέχει εφαρμογή κινητού για συσκευές Android και Apple με Push notifications για alerts και incidents.	ΕΠΙΘΥΜΗΤΟ		
1.1.30	Η προτεινόμενη λύση πρέπει να παρέχει δυνατότητα αυτόματης δημιουργίας profiles/baselines για χρήστες και μηχανές, καθώς και δυνατότητα ανάλυσης της συμπεριφοράς τους μέσω **UEBA** (User and Entity Behavior Analytics). Απαιτείται αναλυτική περιγραφή του τρόπου με τον οποίο παρέχεται η λειτουργικότητα UEBA στο πλαίσιο της προτεινόμενης λύσης.	ΝΑΙ		
1.1.31	Η προτεινόμενη λύση πρέπει να αξιοποιεί μοντέλα **Machine L**earning και **Artificial Intelligence** για τη συνεχή δημιουργία και επικαιροποίηση baseline συμπεριφοράς χρηστών και οντοτήτων, καθώς και για τον εντοπισμό ανωμαλιών. Η λύση πρέπει να εντοπίζει αποκλίσεις από τη φυσιολογική συμπεριφορά, να αναγνωρίζει πιθανές αιτίες και να δημιουργεί alerts, ώστε να υποστηρίζεται η έγκαιρη διερεύνηση πιθανών απειλών.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1.32	Η προτεινόμενη λύση πρέπει να υποστηρίζει integration με Active Directory για τον έλεγχο των user accounts αναφορικά με τα πιο κάτω: • Inactive users • Nested groups • Successful και unsuccessful login attempts • Expired codes • Soon to-expire passwords Η λύση πρέπει να παρέχει δυνατότητα ελέγχου του Active Directory περιβάλλοντος μέσω κεντρικής κονσόλας διαχείρισης. Ο Ανάδοχος υποχρεούται να περιλάβει στο πλαίσιο της προσφερόμενης λύσης οποιαδήποτε σχετική άδεια χρήσης (license) απαιτείται για την κάλυψη της ανωτέρω λειτουργικότητας.	ΕΠΙΘΥΜΗΤΟ		
1.1.33	Η προτεινόμενη λύση πρέπει να υποστηρίζει την εγκατάσταση endpoint agents για τη συλλογή τηλεμετρίας. Τα endpoint agents οφείλουν να παρέχουν τις ακόλουθες δυνατότητες: • File Integrity Monitoring • Application Control • Yara Rules • Enhanced Endpoint Isolation • Enhanced User and Entity Behaviour Analytics • Εντοπισμός security patches που λείπουν Οι endpoint agents πρέπει να παρέχουν τη δυνατότητα διαχείρισης τους μέσω της πλατφόρμας. Οποιαδήποτε σχετική άδεια πρέπει να παρέχεται ως μέρος της προσφερόμενης λύσης.	ΝΑΙ		
1.1.34	Η προτεινόμενη λύση πρέπει να παρέχει ενιαίο graphical user interface για λειτουργίες διαχείρισης ασφάλειας και κινδύνων, συγκεντρώνοντας event/log data και alerts από όλα τα on-premise, private cloud και public cloud περιβάλλοντα σε ένα ενιαίο dashboard.	ΝΑΙ		
1.1.35	Η προτεινόμενη λύση πρέπει να παρέχει προσαρμόσιμους πίνακες ελέγχου με διαμορφώσιμα widgets και συντομεύσεις για παροχή άμεσης πρόσβασης σε incidents, alerts και assets.	ΝΑΙ		
1.1.36	Η προτεινόμενη λύση πρέπει να παρέχει έλεγχο πρόσβασης βάσει ρόλων (RBAC). Πρέπει να υποστηρίζει προκαθορισμένους ρόλους (π.χ., Chief Security Officer, Chief Information Officer, Auditor, Incident Handler, Escalation Engineer) και να επιτρέπει	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τη δημιουργία προσαρμοσμένων ρόλων στις ανάγκες του πελάτη.			
1.1.37	Η προτεινόμενη λύση πρέπει να υποστηρίζει παρακολούθηση απόδοσης και διαθεσιμότητας για συσκευές δικτύου, συστήματα και συνδέσμους επικοινωνίας μέσω της συλλογής και ανάλυσης δεδομένων NetFlow και SNMP. Η λύση πρέπει να παρέχει αναφορά των βασικών μετρήσεων, συμπεριλαμβανομένης της κατάστασης δικτύου και χρήσης πόρων (CPU, μνήμη, δίσκος).	ΝΑΙ		
1.1.38	Η προτεινόμενη λύση πρέπει να υποστηρίζει τη συσχέτιση πολλαπλών alerts σε ένα incident.	ΝΑΙ		
1.1.39	Η προτεινόμενη λύση πρέπει να παρέχει δυνατότητες δημιουργίας αναφορών (reporting) με υποστήριξη προκαθορισμένων προτύπων (predefined templates) για security auditing, compliance και executive reporting. Παράλληλα, πρέπει να υποστηρίζει τη δημιουργία custom reports βάσει των απαιτήσεων του πελάτη. Η λύση πρέπει να υποστηρίζει προγραμματισμό δημιουργίας αναφορών (report scheduling), αυτοματοποιημένη αποστολή μέσω email προς τους χρήστες της πλατφόρμας, καθώς και δυνατότητα εξαγωγής αναφορών σε μορφή CSV και PDF.	ΝΑΙ		
1.1.40	Η προτεινόμενη λύση πρέπει να υποστηρίζει παρακολούθηση συμμόρφωσης με εφαρμοστέα πρότυπα και κανονισμούς, συμπεριλαμβανομένων των ISO 27001 και GDPR.	ΝΑΙ		
1.1.41	Η προτεινόμενη λύση πρέπει να παρακολουθεί τη συνδεσιμότητα των πηγών logs και να εντοπίζει, σε σχεδόν πραγματικό χρόνο, περιπτώσεις κατά τις οποίες πηγές των logs διακόπτουν την αποστολή δεδομένων προς την πλατφόρμα SIEM. Η λύση πρέπει να δημιουργεί αυτοματοποιημένα incidents όταν δεν λαμβάνονται τα αναμενόμενα logs από συγκεκριμένο asset. Για πηγές logs που παύουν να αποστέλλουν logs ή τίθενται εκτός λειτουργίας (offline), ο Ανάδοχος πρέπει να υποστηρίζει τη δημιουργία σχετικού incident εντός πέντε (5) λεπτών.	ΝΑΙ		
1.1.42	Η προτεινόμενη λύση πρέπει να παρέχει τη δυνατότητα ταξινόμησης των IT Assets με βάση το επίπεδο κρισιμότητας τους.	ΝΑΙ		
1.1.43	Στο πλαίσιο της προτεινόμενης λύσης πρέπει να παρέχεται πρόσβαση σε portal, τα οποία θα περιλαμβάνουν πλήρη παρακολούθηση και ιστορικό ενεργειών, οργανωμένα σε timeline view (π.χ. χρόνος ανάθεσης), το οποίο θα αποτυπώνει το σύνολο των ενεργειών που εκτελέστηκαν από τους SOC αναλυτές κατά τη διαδικασία incident response, καθώς και όλες	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	τις ενέργειες που εκτελέστηκαν από χρήστες της Αναθέτουσας Αρχής.			
1.1.44	Ο Ανάδοχος πρέπει να παρέχει κατάλογο των υποστηριζόμενων assets (log sources), επιβεβαιώνοντας παράλληλα ότι το σύνολο των assets που περιλαμβάνονται στο πεδίο εφαρμογής της Αναθέτουσας Αρχής θα υποστηρίζεται από την πλατφόρμα SIEM.	ΝΑΙ		
1.1.45	Η προτεινόμενη λύση πρέπει να υποστηρίζει native playbook δυνατότητες, παρέχοντας προκαθορισμένες, αυτοματοποιημένες ροές εργασίας για την αντιμετώπιση απειλών όπως malware, phishing, unauthorized access και ανώμαλης συμπεριφοράς, όπου αυτό εφαρμόζεται.	ΝΑΙ		
1.1.46	Η προτεινόμενη λύση πρέπει να υποστηρίζει την συνδυαστική ενσωμάτωση δυνατοτήτων **Generative AI και Agentic AI**, βασισμένων σε Large Language Models (**LLMs**) ή ισοδύναμων τεχνολογιών. Οι δυνατότητες Generative AI οφείλουν να υποστηρίζουν τα ακόλουθα: • Αυτόματη σύνοψη των ειδοποιήσεων • Δημιουργία αφηγηματικής περιγραφής της απειλής και χρονολογικής απεικόνισης • Εμπλουτισμό των alerts με συμφραζόμενη πληροφορία • Ερμηνεία δεδομένων από logs, alerts και δεδομένων των αναλυτών • Παροχή προτάσεων για ενέργειες αποκατάστασης Οι δυνατότητες Agentic AI οφείλουν να υποστηρίζουν τα ακόλουθα: • Αυτόνομη ανίχνευση ανωμαλιών και δημιουργία υποθέσεων • Αυτοματοποιημένη έναρξη διερεύνησης • Ιεράρχηση ειδοποιήσεων και ενέργειες απόκρισης, αυτόνομες ενέργειες περιορισμού (π.χ απομόνωση τερματικού σημείου)	ΝΑΙ		
1.1.47	Η επεξεργασία των AI δυνατοτήτων πρέπει να φιλοξενείται εντός της υποδομής Κέντρου Δεδομένων του παρόχου SIEM, χωρίς καμία λειτουργική εξάρτηση από τρίτους παρόχους.	ΕΠΙΘΥΜΗΤΟ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.1.48	Οι δυνατότητες AI οφείλουν να υποστηρίζουν μηχανισμούς συνεχούς μάθησης, βασισμένους σε ανατροφοδότηση (feedback) από την υπηρεσία SOC.	ΝΑΙ		
1.1.49	Η προτεινόμενη λύση πρέπει να χρησιμοποιεί δυνατότητες AI με στόχο την υποστήριξη της μείωσης του Mean Time to Response (MTTR) στα περιστατικά ασφαλείας (incidents).	ΝΑΙ		
1.1.50	Η προτεινόμενη λύση πρέπει να εξασφαλίζει ανθρώπινη εποπτεία και λογοδοσία στις αυτοματοποιημένες λειτουργίες και οδηγούμενες από AI.	ΝΑΙ		
1.1.51	Η δοθεί περιγραφή των μηχανισμών για την παρακολούθηση συμβατικών υποχρεώσεων, συμπεριλαμβανομένου του Service Level Agreement (SLA).	ΝΑΙ		
1.1.52	Η προτεινόμενη λύση πρέπει να υποστηρίζει εργαλεία διαχείρισης ευπαθειών (Vulnerability Management Tools), με την εισαγωγή αποτελεσμάτων σάρωσης από εργαλεία αξιολόγησης ευπαθειών τρίτων κατασκευαστών. Η λύση πρέπει να υποστηρίζει την παρακολούθηση και διαχείριση δραστηριοτήτων αποκατάστασης ευπαθειών, να συσχετίζει ευπάθειες και αδυναμίες διαμόρφωσης με ενεργές απειλές και να υποστηρίζει την ιεράρχηση δράσεων μετριασμού βάσει κινδύνου.	ΝΑΙ		
1.1.53	Η λύση SIEM πρέπει να υποστηρίζει αυτοματοποιημένη ιεράρχηση όλων των ανιχνεύσεων μέσω ευφυούς μηχανισμού Risk Scoring, ο οποίος να λαμβάνει υπόψη τον επιχειρησιακό αντίκτυπο, το επίπεδο εμπιστοσύνης της ανίχνευσης, τη συσχέτιση με MITRE ATT&CK και το πελατοκεντρικό πλαίσιο. Οι ειδοποιήσεις πρέπει να δρομολογούνται αυτόματα σε αναλυτές SOC επιπέδου L1, L2 ή L3 βάσει σοβαρότητας, εξειδίκευσης και τρέχοντος φόρτου εργασίας.	ΝΑΙ		
1.1.54	Το σύστημα πρέπει να διασφαλίζει ότι, σε περίπτωση απώλειας σύνδεσης μεταξύ του Log Collector και της υπηρεσίας, ο Log Collector απαιτείται να συνεχίζει απρόσκοπτα τη συλλογή και τοπική αποθήκευση των καταγραφών (logs). Με την αποκατάσταση της σύνδεσης, το σύστημα πρέπει να προωθεί αυτόματα και με ασφάλεια το σύνολο των αποθηκευμένων δεδομένων προς τα data centers για επεξεργασία, διασφαλίζοντας ότι δεν θα υπάρξει απώλεια δεδομένων λόγω διακοπής σύνδεσης ή υπηρεσίας.	ΝΑΙ		
1.2	**Threat Intelligence**			

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.2.1	Η προτεινόμενη λύση πρέπει να περιλαμβάνει πληροφόρηση που παρέχει λεπτομερείς πληροφορίες για απειλές και στοχευμένες οδηγίες αντιμετώπισης, εμπλουτισμένες μέσω τροφοδοσιών threat intelligence.	ΝΑΙ		
1.2.2	Η λύση πρέπει να υποστηρίζει την συνεχή ενσωμάτωση τουλάχιστον δύο (2) τροφοδοσιών threat intelligence ανοιχτού κώδικα εντός της πλατφόρμας.	ΝΑΙ		
1.2.3	Η λύση πρέπει να υποστηρίζει την συνεχή ενσωμάτωση τουλάχιστον δύο (2) εμπορικών τροφοδοσιών threat intelligence εντός της πλατφόρμας.	ΝΑΙ		
1.2.4	Η λύση πρέπει να περιλαμβάνει και να διατηρεί μια εσωτερική βάση δεδομένων Threat Intelligence για να συμπληρώνει τις ενσωματωμένες εξωτερικές threat intelligence τροφοδοσίες.	ΝΑΙ		
1.3	**Τεχνολογία Κυβερνοπαγίδων και χρήση αυτής**			
1.3.1	Η προτεινόμενη λύση πρέπει να παρέχει δυνατότητες ανίχνευσης μετά από παραβίαση για την ανίχνευση κίνησης και κακόβουλης δραστηριότητας χρησιμοποιώντας τεχνολογία εξαπάτησης (deception). Οποιαδήποτε σχετική άδεια πρέπει να παρέχεται ως μέρος της προσφερόμενης λύσης.	ΝΑΙ		
1.3.2	Η αδειοδότηση της τεχνολογία κυβερνοπαγίδων θα υποστηρίζει τουλάχιστον 10 κυβερνοπαγίδες.	ΝΑΙ		
1.3.3	Οι κυβερνοπαγίδες θα αναπτυχθούν με σκοπό την προληπτική ανίχνευση οποιασδήποτε «επίθεσης» και «επιτιθέμενων» κατά του οργανισμού. Να αναφερθούν δυνατότητες.	ΝΑΙ		
1.3.4	Οι κυβερνοπαγίδες θα πρέπει να είναι ικανές να δελεάσουν τον επιτιθέμενο με σκοπό την πλήρη εξαπάτηση και τον εντοπισμό του. Να αναφερθούν οι τρόποι εξαπάτησης.	ΝΑΙ		
1.3.5	Οι κυβερνοπαγίδες σε περίπτωση εντοπισμού κακόβουλης χρήσης από επιτιθέμενο, θα πρέπει να δημιουργούν ειδοποιήσεις (alert) στη λύση SIEM του Αναδόχου.	ΝΑΙ		
1.3.6	Οι αναλυτές του Επιχειρησιακού Κέντρου Ασφαλείας του Αναδόχου, θα πρέπει να χρησιμοποιούν τις πληροφορίες που παρέχει η τεχνολογία των κυβερνοπαγίδων και να παρέμβουν, με σκοπό την ανάλυσή της επίθεσης και της αντιμετώπισής της.	ΝΑΙ		
1.3.7	Η πλατφόρμα SIEM του Αναδόχου, θα πρέπει να παρέχει πληροφορίες για τη χρήση της τεχνολογίας κυβερνοπαγίδων.	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
1.4	**ΥΠΗΡΕΣΙΑ SOC**			
1.4.1	Ο πάροχος απαιτείται να περιγράψει πώς λειτουργεί το Security Operations Centre (SOC) σε 24/7/365 βάση, μαζί με τις ρυθμίσεις στελέχωσης (L1-L3 Αναλυτές). Το Security Operations Centre πρέπει να λειτουργεί εντός της Ελλάδας.	ΝΑΙ		
1.4.2	Ο Ανάδοχος απαιτείται να περιγράψει τη διαδικασία πρόσληψης προσωπικού για τη διατήρηση υψηλών προτύπων ποιότητας για το Security Operations Centre. Πρέπει να περιγραφεί η διαδικασία ελέγχου ιστορικού τους και η συνεχής ανάπτυξη της γνώσης και δυνατοτήτων τους.	ΝΑΙ		
1.4.3	Κάθε ειδοποίηση που δημιουργείται πρέπει να αναλύεται και να ερευνάται από εξειδικευμένο προσωπικό (Cyber Security Analysts) του Αναδόχου, να καταγράφεται και να παρακολουθείται σε λίστα διαχείρισης ειδοποιήσεων προσβάσιμη από τον ανάδοχο και τον πελάτη.	ΝΑΙ		
1.4.4	Το προσωπικό του SOC πρέπει να αποτελείται από αναλυτές που λειτουργούν βάση 24/7/365 (Cybersecurity Analysts L1, L2, L3) και να εποπτεύονται από Team Leaders. Ο Ανάδοχος πρέπει να παρέχει αναλυτική περιγραφή των αρμοδιοτήτων στελέχωσης για κάθε επίπεδο αναλυτή.	ΕΠΙΘΥΜΗΤΟ		
1.4.5	Οι υπηρεσίες SOC δεν πρέπει να παρέχεται από τρίτους (υπεργολάβους).	ΝΑΙ		
1.4.6	Η υπηρεσία πρέπει να υποστηρίζει συνεχή λειτουργική μάθηση για τη βελτίωση της ανίχνευσης, απόκρισης και αποτελεσματικότητας των επιχειρήσεων ασφαλείας.	ΝΑΙ		
1.4.7	Η υπηρεσία πρέπει να υποστηρίζει δυνατότητες μείωσης του alert noise και ελαχιστοποίησης των false positives με την πάροδο του χρόνου.	ΝΑΙ		
1.4.8	Η υπηρεσία πρέπει να επιβάλλει ανθρώπινη έγκριση σε καθορισμένα κρίσιμα σημεία ελέγχου για ενέργειες υψηλού κινδύνου ή ευαίσθητες αυτοματοποιημένες ενέργειες.	ΝΑΙ		
1.4.9	Η υπηρεσία πρέπει να υποστηρίζει δομημένες δυνατότητες threat hunting, βασισμένες σε υποθέσεις (hypothesis-driven).	ΝΑΙ		
1.4.10	Οι λειτουργίες threat hunting οφείλουν να υποστηρίζονται από contextualized telemetry δεδομένα και πηγές από threat intelligence feeds.	ΝΑΙ		
1.4.11	Η υπηρεσία SOC πρέπει να ενσωματώνει δυνατότητες AI για την υποστήριξη της ανάλυσης των alerts και της	ΝΑΙ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	διερεύνησης περιστατικών, με στόχο τη μείωση του Mean Time to Response (MTTR).			
1.4.12	Η Αναθέτουσα Αρχή διατηρεί το δικαίωμα να πραγματοποιεί επισκέψεις στις εγκαταστάσεις του παρόχου υπηρεσιών SOC για σκοπούς ελέγχου (audit). Ο Ανάδοχος πρέπει να υποστηρίζει τις εν λόγω επισκέψεις στο πλαίσιο της παροχής των υπηρεσιών του.	ΝΑΙ		
1.4.13	Ο πάροχος πρέπει να περιγράψει τις πολιτικές, διαδικασίες και ελέγχους που υπάρχουν για τη διαφύλαξη του απορρήτου και της εμπιστευτικότητας των δεδομένων του πελάτη.	ΝΑΙ		
1.4.14	Ο πάροχος πρέπει να περιγράψει τις διαδικασίες ελέγχου ασφάλειας που διατηρούνται για το περιβάλλον SOC.	ΝΑΙ		
1.4.15	Ο πάροχος πρέπει να διαθέτει σύστημα ticketing για την καταγραφή, κατηγοριοποίηση και αναφορά των περιστατικών ασφαλείας (incidents) και να εξασφαλίζει τη σωστή και έγκαιρη ειδοποίηση της σχετικής ομάδας του οργανισμού. Σαφείς και λεπτομερείς οδηγίες περιορισμού και αποκατάστασης πρέπει να δίνονται σε κάθε περιστατικό.	ΝΑΙ		
1.4.16	Ο πελάτης πρέπει να έχει πρόσβαση στα ίδια στοιχεία με τους αναλυτές SOC όσο αφορά την ανάλυση περιστατικών.	ΝΑΙ		
1.4.17	Ο πάροχος πρέπει να παρέχει τακτική αναφορά για δραστηριότητες ασφαλείας, συμβάντα και περιστατικά. Οι δυνατότητες διαχείρισης περιστατικών πρέπει να περιλαμβάνουν καθορισμένες ροές κλιμάκωσης, παρακολούθηση περιστατικών και ορατότητα κατάστασης, και προτάσεις αποκατάστασης για την υποστήριξη αποτελεσματικής επίλυσης περιστατικών.	ΝΑΙ		
1.4.18	Ο πάροχος πρέπει να διεξάγει αξιολόγηση αρχιτεκτονικής (Architecture Reviews) κατά τη φάση ενσωμάτωσης και ανά εξάμηνο για την αξιολόγηση της υποδομής του πελάτη, τον εντοπισμό κενών ορατότητας και κινδύνων ασφαλείας.	ΕΠΙΘΥΜΗΤΟ		
1.4.19	Ο πάροχος πρέπει να διεξάγει τριμηνιαία Service Delivery Reviews με τα βασικά ενδιαφερόμενα μέρη τόσο από την υπηρεσία SOC όσο και από τον πελάτη για αναθεώρηση της υπηρεσίας, παρουσίασης πρόσφατων περιστατικών, δραστηριοτήτων αποκατάστασης και ορατότητας έκθεσης σε κινδύνους. Επιπρόσθετα, στις συναντήσεις θα πρέπει να παρουσιάζονται ενδείξεις απόδοσης της υπηρεσίας, με κάποια ενδεικτικά παραδείγματα όπως:	ΕΠΙΘΥΜΗΤΟ		

Α/Α	ΠΕΡΙΓΡΑΦΗ / ΠΡΟΔΙΑΓΡΑΦΕΣ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
	• Μέσος Χρόνος Ανίχνευσης Συμβάντων (MTTD – Mean Time to Detect) • Μέσος Χρόνος Απόκρισης (MTTR – Mean Time to Respond) • Ποσοστό Ψευδώς Θετικών (False Positive Rate) • Όγκος και Κατηγοριοποίηση Συμβάντων ανά επίπεδο σοβαρότητας (Severity Levels) • Πλήθος συμβάντων ανά πηγή (endpoint, firewall, cloud, identity κ.λπ.) • SLA συμμόρφωσης απόκρισης περιστατικών			
1.4.20	Η υπηρεσία SOC πρέπει να καταγράφει το αποτέλεσμα της ανάλυσης όλων των alerts, συμπεριλαμβανομένων των alerts που ταξινομούνται ως false positives, με σκοπό τη διατήρηση audit trail των δραστηριοτήτων SOC και την υποστήριξη βάσης δεδομένων των incidents.	ΝΑΙ		
1.4.21	Η Αναθέτουσα Αρχή πρέπει να διαθέτει ασφαλή online πρόσβαση στην προσφερόμενη πλατφόρμα του Αναδόχου, για την παρακολούθηση των incidents. Η πρόσβαση πρέπει να υλοποιείται με χρήση two-factor authentication για ενισχυμένη προστασία.	ΝΑΙ		
1.4.22	Η υπηρεσία πρέπει να επιτρέπει την επιλογή διαφορετικών επαφών κλιμάκωσης (escalation contacts) βάσει τύπου ειδοποίησης και επιπέδου επικινδυνότητας. Οι επαφές αυτές οφείλουν να περιλαμβάνουν υποχρεωτικά αριθμό τηλεφώνου για τη διαχείριση των high και critical incidents.	ΝΑΙ		
1.4.23	Τα περιστατικά ασφαλείας (incidents) πρέπει να παρέχονται και να κατηγοριοποιούνται σε τέσσερις διακριτές ομάδες: 1. Κρίσιμα (Critical) 2. Υψηλά (High) 3. Μεσαία (Medium) 4. Ενημερωτικά (Informative)	ΝΑΙ		
1.4.24	Η υπηρεσία πρέπει να *εγγυείται χρόνους απόκρισης* (SLAs) ανάλογα με τη σοβαρότητα των περιστατικών όπως φαίνονται παρακάτω: 1. Κρίσιμα (Critical) 0:30:00 - 1:00:00 2. Υψηλά (High) 1:00:00 - 3:00:00 3. Μεσαία (Medium) 3:00:00 - 6:00:00	ΝΑΙ		

2. Λογισμικό Security, Orchestration, Automation, And Response

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.1	**Security Orchestration, Automation and Response - SOAR**			
2.1.1	Απαιτούνται δυνατότητες Security Orchestration, Automation and Response (**SOAR**), διασφαλίζοντας την υλοποίηση των πιο κάτω λειτουργιών απευθείας μέσω της πλατφόρμας SIEM: • Προσθήκη Firewall Policies • Απομόνωση endpoints ➢ Aggressive Isolation – Πλήρης αποσύνδεση του endpoint από το δίκτυο, με άμεσο τερματισμό όλων των επικοινωνιών, συμπεριλαμβανομένης της επικοινωνίας με την πλατφόρμα ➢ Soft Isolation – Διακοπή κάθε σύνδεσης προς το Endpoint, εκτός από τη σύνδεση με την πλατφόρμα SIEM Απενεργοποίηση χρηστών (user suspension) στο Active Directory	ΝΑΙ		
2.1.2	Οι δυνατότητες SOAR πρέπει να είναι εγγενώς ενσωματωμένες στην πλατφόρμα του SIEM, χωρίς να απαιτείται ξεχωριστή άδεια χρήσης ή προϊόν τρίτου κατασκευαστή. Όλες οι άδειες λειτουργίας πρέπει να περιλαμβάνονται.	ΕΠΙΘΥΜΗΤΟ		
2.1.3	Οι ενέργειες που εκτελούνται μέσω SOAR οφείλουν να προβάλλονται σε live feed εντός της πλατφόρμας SIEM.	ΝΑΙ		
2.1.4	Πρέπει να παρέχεται από την πλατφόρμα δυνατότητα παρακολούθησης μέσω live feed και ιστορικής απεικόνισης, ολοκληρωμένη ανάλυση της δραστηριότητας και της συμπεριφοράς που σχετίζεται με blocked IPs, suspended users και isolated endpoints για προκαθορισμένο χρονικό διάστημα.	ΝΑΙ		
2.1.5	Απαιτείται οι SOAR ενέργειες να παρέχουν δυνατότητα πλήρους αυτοματοποίησης μέσω ενσωμάτωσης με correlation rules και playbooks.	ΝΑΙ		

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
2.1.6	Η απόκριση SOAR πρέπει να είναι πλήρως ενσωματωμένη εντός της διαδικασίας διαχείρισης των incidents, για ταχύτερη απόκριση απευθείας από το μενού διαχείρισης περιστατικών.	ΝΑΙ		
2.1.7	Απαιτείται ο πίνακας ελέγχου SOAR να απεικονίζει με σαφήνεια την πηγή δημιουργίας κάθε SOAR ενέργειας, όπως χειροκίνητης ενέργειας χρήστη/αναλυτή ή αυτοματοποίησης μέσω correlation rule.	ΝΑΙ		
2.1.8	Οι SOAR ενέργειες πρέπει να έχουν τη δυνατότητα να ενεργοποιηθούν άμεσα είτε με προγραμματισμό σε καθορισμένη ημερομηνία.	ΝΑΙ		