# ΠΙΝΑΚΑΣ ΑΠΑΝΤΗΣΕΩΝ ΣΕ ΣΧΟΛΙΑ ΚΑΙ ΑΙΤΗΜΑΤΑ ΔΙΕΥΚΡΙΝΙΣΕΩΝ ΠΡΟΣΦΕΡΟΝΤΩΝ

Διαγωνισμός για την παροχή Υπηρεσιών SIEM / SOC και EDR / XDR —

Ερωτήματα (που υποβλήθηκαν μέχρι 8/9/2026) και αφορούν το Παράρτημα 2, Έντυπο Τεχνικών Προδιαγραφών

## 1. Σκοπός του παρόντος

Το παρόν έγγραφο εκδίδεται από την Αναθέτουσα Αρχή σε απάντηση των σχολίων και αιτημάτων διευκρινίσεων που υποβλήθηκαν από ενδιαφερόμενους οικονομικούς φορείς επί του Παραρτήματος 2 (Έντυπο Τεχνικών Προδιαγραφών). Κοινοποιείται στο σύνολο των ενδιαφερόμενων οικονομικών φορέων, σύμφωνα με τις αρχές της ίσης μεταχείρισης και της διαφάνειας.

Όπου στον κατωτέρω πίνακα αναφέρεται νέα διατύπωση προδιαγραφής, αυτή αντικαθιστά την αντίστοιχη υφιστάμενη διατύπωση του Παραρτήματος 2 και υπερισχύει αυτής. Το σύνολο των μεταβολών ενσωματώνεται σε αναθεωρημένη έκδοση του Παραρτήματος 2, η οποία εκδίδεται ταυτόχρονα με το παρόν.

## 2. Συνοπτική εικόνα

Επί συνόλου είκοσι τριών (23) σημείων που τέθηκαν:

- Γίνονται πλήρως αποδεκτά: 14 σημεία.
- Γίνονται μερικώς αποδεκτά, με αναδιατύπωση: 8 σημεία.
- Δεν γίνονται αποδεκτά: 1 σημείο (Ενότητα 3.2 – SOC Staffing).

Η πλειονότητα των βάσιμων παρατηρήσεων αφορά σημεία στα οποία η προδιαγραφή περιέγραφε συγκεκριμένο τρόπο υλοποίησης αντί για το επιδιωκόμενο αποτέλεσμα. Τα σημεία αυτά αναδιατυπώνονται σε βάση αποτελέσματος (outcome-based), χωρίς μείωση του απαιτούμενου επιπέδου ασφάλειας. Σε ορισμένες περιπτώσεις η αναδιατύπωση ενισχύει τις απαιτήσεις, ιδίως ως προς την ελεγχόμενη διανομή ενημερώσεων και τη διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ.

## 3. Ουσιώδεις τροποποιήσεις και προθεσμία

Τα σημεία 2, 3, 11, 17 και 23 συνιστούν ουσιώδεις μεταβολές των εγγράφων του διαγωνισμού. Ειδικότερα, η συμπλήρωση των στοιχείων sizing (σημείο 23) επηρεάζει άμεσα τη δυνατότητα κοστολόγησης. Για τον λόγο αυτό εξετάζεται παράταση της προθεσμίας υποβολής προσφορών, η οποία θα ανακοινωθεί με χωριστό έγγραφο.

## 4. Επεξήγηση κατηγοριών απόφασης

ΑΠΟΔΕΚΤΟ: το αίτημα γίνεται δεκτό και η προδιαγραφή τροποποιείται αναλόγως. ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ: το αίτημα γίνεται δεκτό ως προς ορισμένα σκέλη· διατηρούνται ή αναδιατυπώνονται απαιτήσεις που απορρέουν από το κανονιστικό πλαίσιο ή από ουσιαστική ανάγκη της Αναθέτουσας Αρχής. ΔΙΕΥΚΡΙΝΙΣΗ: παρέχεται ερμηνεία της υφιστάμενης απαίτησης, με ή χωρίς οριοθέτηση του αντικειμένου. ΔΕΝ ΓΙΝΕΤΑΙ ΑΠΟΔΕΚΤΟ: το αίτημα απορρίπτεται με αιτιολόγηση.

## 5. Πίνακας απαντήσεων ανά σημείο

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 1 | **Ενότητα Α – Α/Α 3 Πιστοποιήσεις (σελ. 1)** | Αντίφαση μεταξύ προδιαγραφής («SOC 2 ή ισοδύναμη») και αποδεικτικού στοιχείου (υποχρεωτικό SOC 2). Ζητείται η αφαίρεση της υποχρεωτικής απαίτησης SOC 2 και η αποδοχή ISO/IEC 27001. | **ΑΠΟΔΕΚΤΟ** | Επιβεβαιώνεται η ύπαρξη ασυμφωνίας μεταξύ της προδιαγραφής και του απαιτούμενου αποδεικτικού στοιχείου. Το SOC 2 αποτελεί έκθεση διασφάλισης (attestation) και όχι πιστοποίηση, και ως εκ τούτου δεν διατηρείται ως κριτήριο αποκλεισμού. | Η προδιαγραφή τροποποιείται ως εξής:<br>(α) Υποχρεωτικό: εν ισχύι πιστοποιητικό ISO/IEC 27001 του νομικού προσώπου που θα παρέχει την υπηρεσία (όχι μόνο σε επίπεδο ομίλου), με πεδίο εφαρμογής που καλύπτει ρητά τις υπηρεσίες SOC/MSSP.<br>(β) Βαθμολογούμενο (μη αποκλειστικό): SOC 2 Type II ή ισοδύναμη έκθεση ανεξάρτητης διασφάλισης, ISO/IEC 27017, ISO/IEC 27018, ISO 22301.<br>Το αποδεικτικό στοιχείο του Α/Α 3 αναδιατυπώνεται αναλόγως. |
| 2 | **Ενότητα Α – Α/Α 2 Κατάλογος Έργων (σελ. 1)** | Το ποσό €11.000.000 στο αποδεικτικό στοιχείο θεωρείται τυπογραφικό λάθος· ζητείται επιβεβαίωση ότι το ορθό είναι €1.000.000, όπως αναφέρεται στην Προδιαγραφή. | **ΑΠΟΔΕΚΤΟ** | Επιβεβαιώνεται ότι πρόκειται για εκ παραδρομής τυπογραφικό σφάλμα. Επειδή το σημείο αφορά κριτήριο ποιοτικής επιλογής, η διόρθωση πραγματοποιείται με επίσημη τροποποίηση των εγγράφων του διαγωνισμού και όχι με απλή διευκρίνιση. | Το ποσό διορθώνεται σε €1.000.000. Διατύπωση: «Τουλάχιστον τρία (3) συναφή έργα SIEM/SOC ή/και EDR/XDR, υλοποιημένα ή σε λειτουργία εντός της τελευταίας πενταετίας, συνολικής αξίας τουλάχιστον €1.000.000.»<br>Η διόρθωση κοινοποιείται σε όλους τους ενδιαφερόμενους οικονομικούς φορείς. |
| 3 | **Ενότητα Α – Α/Α 4 EU / Sovereign Requirements (σελ. 1–2)** | Ο συνδυασμός ιδιοκτησίας vendor εντός ΕΕ, αποκλειστικά EU-based operations και υποχρεωτικού EKM/HYOK θεωρείται περιοριστικός. Ζητείται αντικατάσταση με | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό ότι η απαίτηση περί μετοχικής ιδιοκτησίας του κατασκευαστή εντός ΕΕ είναι δυσανάλογη και αποσύρεται. Δεν γίνονται δεκτές οι λοιπές χαλαρώσεις: οι απαιτήσεις τοπικότητας δεδομένων, απομόνωσης και ελέγχου κλειδιών | ΑΠΟΣΥΡΕΤΑΙ: απαίτηση ιδιοκτησίας/μετοχικής σύνθεσης του κατασκευαστή εντός ΕΕ.<br>ΠΑΡΑΜΕΝΟΥΝ ΥΠΟΧΡΕΩΤΙΚΑ:<br>• Αποθήκευση και επεξεργασία δεδομένων αποκλειστικά εντός ΕΕ/ΕΟΧ (at rest και in process), περιλαμβανομένων backups και DR sites. |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| | | απαιτήσεις EU data residency, GDPR, encryption, access control και συμβατικές διασφαλίσεις. | | απορρέουν από τις υποχρεώσεις της Αναθέτουσας Αρχής ως εποπτευόμενης οντότητας (DORA, άρθρα 28–30) και από την ευαισθησία των δεδομένων που τυγχάνουν επεξεργασίας. | • Λειτουργίες L1/L2 και υποστήριξη από προσωπικό εγκατεστημένο εντός ΕΕ/ΕΟΧ.<br>• Λογική απομόνωση tenant (single-tenant ή τεκμηριωμένη logical isolation).<br>• Customer-Managed Keys (BYOK/CMK) με δυνατότητα ανάκλησης από την Αναθέτουσα Αρχή.<br>• Πλήρης κατάλογος υπεργολάβων/υπο-επεξεργαστών και υποχρέωση προηγούμενης ενημέρωσης επί μεταβολών.<br>• Συμβατικό δικαίωμα ελέγχου και πρόσβασης εποπτικής αρχής (ΚΤΚ) κατά DORA.<br>• Υποχρέωση ειδοποίησης σε περίπτωση αιτήματος πρόσβασης από αρχή τρίτης χώρας, στο μέτρο που επιτρέπεται από τον νόμο.<br>ΒΑΘΜΟΛΟΓΟΥΜΕΝΟ (μη αποκλειστικό): HYOK / External Key Management. |
| 4 | **Ενότητα Α – Α/Α 6**<br>**Τοποθεσία SOC (σελ. 2)** | Η υποχρεωτική εγκατάσταση του SOC στην Κύπρο αποκλείει MSSPs με πιστοποιημένα 24x7 SOCs σε άλλα κράτη μέλη. Ζητείται αποδοχή SOC εντός ΕΕ. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτή η λειτουργία SOC εντός ΕΕ/ΕΟΧ. Διατηρούνται ωστόσο απαιτήσεις που διασφαλίζουν την επιχειρησιακή επάρκεια και την τοπική ανταπόκριση σε περιστατικό. | Νέα διατύπωση: «Το SOC δύναται να λειτουργεί από οποιοδήποτε κράτος μέλος της ΕΕ/ΕΟΧ, υπό την προϋπόθεση ότι:<br>(α) λειτουργεί 24x7x365 με τεκμηριωμένο shift model και εφεδρεία (δεύτερη τοποθεσία ή τεκμηριωμένο σχέδιο συνέχειας του ίδιου του SOC),<br>(β) τα δεδομένα παραμένουν εντός ΕΕ/ΕΟΧ,<br>(γ) διασφαλίζεται επικοινωνία στην ελληνική γλώσσα σε επίπεδο escalation, service management και αναφορών,<br>(δ) ορίζεται τοπικό σημείο επαφής και δυνατότητα φυσικής παρουσίας στην Κύπρο εντός είκοσι τεσσάρων (24) ωρών σε περιστατικό υψηλής σοβαρότητας.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 5 | **Ενότητα 2.1 – Α/Α 1**<br>**Single Pane of Glass (σελ. 3)** | Ζητείται επιβεβαίωση ότι το «Single Pane of Glass» αφορά ενιαία λειτουργική εικόνα και δεν απαιτεί όλες οι δυνατότητες να προέρχονται από έναν κατασκευαστή. | **ΔΙΕΥΚΡΙΝΙΣΗ – ΑΠΟΔΕΚΤΟ** | Επιβεβαιώνεται. Η απαίτηση αφορά ενιαία επιχειρησιακή/λειτουργική εικόνα προς την Αναθέτουσα Αρχή και όχι μονο-κατασκευαστική αρχιτεκτονική. Γίνεται δεκτή vendor-agnostic αρχιτεκτονική με ενσωμάτωση best-of-breed τεχνολογιών. | Προστίθεται διευκρινιστική παράγραφος: «Γίνεται δεκτή αρχιτεκτονική πολλαπλών κατασκευαστών. Ο Ανάδοχος φέρει ενιαία και αδιαίρετη ευθύνη για τη διασύνδεση, τη λειτουργία, την υποστήριξη και την τήρηση των SLA του συνόλου των επιμέρους τεχνολογιών. Το κόστος και ο κίνδυνος ολοκλήρωσης βαρύνουν αποκλειστικά τον Ανάδοχο. Απαιτείται ενιαία κονσόλα/portal για incidents, alerts, αναφορές και μετρικές SLA.» |
| 6 | **Ενότητα 2.1 – Α/Α 7**<br>**Active Directory Audit (σελ. 4)** | Οι λειτουργίες inactive users, nested groups, password expiry και AD assessment αποτελούν Identity Security δυνατότητες και όχι τυπικές SIEM λειτουργίες. Ζητείται αφαίρεση ή χαρακτηρισμός ως προαιρετικές. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό ότι η απαίτηση δεν αποτελεί τυπική λειτουργία SIEM. Δεν αφαιρείται όμως, καθώς αντιστοιχεί σε πραγματική ανάγκη διαχείρισης κινδύνου ταυτοτήτων. Μετατίθεται από τεχνική προδιαγραφή προϊόντος σε υποχρεωτικό παραδοτέο υπηρεσίας, τεχνολογικά ουδέτερο. | Μεταφέρεται στην ενότητα παραδοτέων υπηρεσίας με διατύπωση: «Ο Ανάδοχος υποχρεούται σε τριμηνιαία αναφορά υγιεινής καταλόγου ταυτοτήτων (Identity/AD Hygiene Report), η οποία κατ' ελάχιστον καλύπτει: ανενεργούς και stale λογαριασμούς, προνομιούχους λογαριασμούς και μεταβολές τους, εμφωλευμένες ομάδες (nested groups), εξαιρέσεις πολιτικής κωδικών και service accounts. Ο τρόπος υλοποίησης (native SIEM, πρόσθετο εργαλείο ή χειροκίνητη ανάλυση) επιλέγεται ελεύθερα από τον προσφέροντα και δεν βαθμολογείται.» |
| 7 | **Ενότητα 2.1 – Α/Α 15**<br>**File Integrity Monitoring (σελ. 6)** | Ζητείται επιβεβαίωση ότι το FIM δεν απαιτείται να παρέχεται native από το SIEM και μπορεί να παρέχεται μέσω EDR ή workload security με προώθηση events στο SIEM. | **ΑΠΟΔΕΚΤΟ** | Επιβεβαιώνεται. Η απαίτηση είναι λειτουργική και όχι αρχιτεκτονική. | Νέα διατύπωση: «Απαιτείται δυνατότητα File Integrity Monitoring σε κρίσιμα συστήματα (κατ' ελάχιστον Domain Controllers, database servers, file servers και συστήματα που φιλοξενούν δεδομένα προσωπικού χαρακτήρα). Το FIM δύναται να παρέχεται native από το SIEM ή μέσω EDR/workload security τεχνολογίας, υπό την προϋπόθεση ότι τα σχετικά γεγονότα προωθούνται στο SIEM για συσχέτιση, alerting και αναφορές, με ενιαία διαχείριση πολιτικών από τον Ανάδοχο.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 8 | **Ενότητα 2.2 – Α/Α 2 AI Capabilities (σελ. 8)** | Ζητείται αφαίρεση της απαίτησης το AI processing να φιλοξενείται στο private data centre του SIEM provider και της απαγόρευσης third-party AI services, με εστίαση σε data residency, confidentiality, isolation και compliance. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Αποσύρεται η απαίτηση φιλοξενίας σε ιδιόκτητο data centre του παρόχου. Δεν χαλαρώνει όμως η ουσία των ελέγχων: η επεξεργασία με τεχνητή νοημοσύνη αφορά δεδομένα ασφάλειας υψηλής ευαισθησίας. | Νέα διατύπωση: «Δυνατότητες τεχνητής νοημοσύνης δύνανται να παρέχονται από native ή third-party υπηρεσίες, εφόσον σωρευτικά:<br>(α) η επεξεργασία πραγματοποιείται εντός ΕΕ/ΕΟΧ,<br>(β) απαγορεύεται ρητά και συμβατικά η χρήση δεδομένων της Αναθέτουσας Αρχής για εκπαίδευση, βελτίωση ή αξιολόγηση μοντέλων,<br>(γ) δηλώνονται όλες οι υπηρεσίες AI και οι υπο-επεξεργαστές που εμπλέκονται,<br>(δ) διασφαλίζεται απομόνωση tenant και έλεγχος πρόσβασης,<br>(ε) υφίσταται δυνατότητα πλήρους απενεργοποίησης των AI λειτουργιών κατόπιν αιτήματος της Αναθέτουσας Αρχής, χωρίς απώλεια της βασικής υπηρεσίας,<br>(στ) τηρείται ο ΓΚΠΔ και ο Κανονισμός (ΕΕ) 2024/1689 για την τεχνητή νοημοσύνη.» |
| 9 | **Ενότητα 2.2 – Α/Α 5 System Availability Monitoring (σελ. 9)** | Ping, SNMP, WMI, routing protocols και infrastructure availability monitoring αποτελούν NOC λειτουργίες. Ζητείται αφαίρεση από το υποχρεωτικό SIEM/SOC scope. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό ότι το γενικό infrastructure availability monitoring αποτελεί λειτουργία NOC. Δεν αφαιρείται ωστόσο η παρακολούθηση υγείας των πηγών καταγραφής, η οποία αποτελεί γνήσια και κρίσιμη απαίτηση SIEM για σκοπούς ελέγχου και συμμόρφωσης. | ΠΑΡΑΜΕΝΕΙ ΥΠΟΧΡΕΩΤΙΚΟ: «Log Source Health Monitoring — αυτόματη ανίχνευση διακοπής ή ανώμαλης μείωσης αποστολής δεδομένων από κάθε πηγή, με alert εντός καθορισμένου χρόνου, ημερήσια επισκόπηση και μηνιαία αναφορά κάλυψης πηγών.»<br>ΜΕΤΑΦΕΡΕΤΑΙ ΣΕ ΠΡΟΑΙΡΕΤΙΚΗ ΥΠΗΡΕΣΙΑ (με χωριστή τιμολόγηση στο έντυπο οικονομικής προσφοράς): γενικό availability monitoring υποδομής (ping, SNMP, WMI, interfaces, routing). |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 10 | **Ενότητα 2.2 – Α/Α 6**<br>**Synthetic Transaction Monitoring (σελ. 9)** | Το synthetic monitoring (HTTP, HTTPS, DNS, LDAP, SMTP, FTP, JDBC) αποτελεί APM/NOC λειτουργικότητα και όχι core SIEM capability. Ζητείται αφαίρεση ή μετατροπή σε optional. | **ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό. Η απαίτηση αφαιρείται από το υποχρεωτικό αντικείμενο SIEM/SOC. | Μεταφέρεται σε προαιρετική υπηρεσία με χωριστή τιμολόγηση. Δεν αποτελεί κριτήριο αποδοχής ούτε βαθμολογείται στην τεχνική αξιολόγηση. |
| 11 | **Ενότητες 2.2 & 2.6**<br>**SIEM Log Retention (σελ. 10 & 12)** | Αντικρουόμενες απαιτήσεις 6 μηνών hot, 12 μηνών hot και 3 μηνών retention. Προτείνεται 3 μήνες hot και 9 μήνες archive. | **ΑΠΟΔΕΚΤΟ ΩΣ ΠΡΟΣ ΤΗΝ ΑΝΤΙΦΑΣΗ – ΔΙΑΦΟΡΕΤΙΚΗ ΡΥΘΜΙΣΗ** | Επιβεβαιώνεται η ύπαρξη αντικρουόμενων απαιτήσεων και ενοποιούνται. Η προτεινόμενη περίοδος των τριών (3) μηνών hot storage κρίνεται ανεπαρκής σε σχέση με τον μέσο χρόνο παραμονής απειλής και τις ανάγκες forensic ανάλυσης και ελέγχου. | Ενιαία διατύπωση που αντικαθιστά κάθε προηγούμενη αναφορά:<br>• Έξι (6) μήνες hot / πλήρως αναζητήσιμα δεδομένα (fully searchable, online).<br>• Επιπλέον έξι (6) μήνες archive/cold retention — συνολική διατήρηση δώδεκα (12) μηνών.<br>• Ανάκτηση αρχειοθετημένων δεδομένων εντός σαράντα οκτώ (48) ωρών από αίτημα, χωρίς πρόσθετη χρέωση για σκοπούς έρευνας περιστατικού, εσωτερικού ελέγχου ή εποπτικού αιτήματος.<br>• Υποχρέωση παράδοσης του συνόλου των δεδομένων σε ανοικτό, μηχαναγνώσιμο μορφότυπο κατά τη λήξη ή καταγγελία της σύμβασης.<br>ΠΡΟΑΙΡΕΤΙΚΑ: χωριστή τιμή για επέκταση σε δώδεκα (12) μήνες hot storage. |
| 12 | **Ενότητα 2.6 – Α/Α 1**<br>**WAF / UTM (σελ. 12)** | Η υποχρεωτική απαίτηση WAF και UTM μπροστά από την υπηρεσία είναι infrastructure-specific και δεν εφαρμόζεται σε vendor-managed SaaS SIEM πλατφόρμες. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό για πλατφόρμες SaaS που παρέχονται από τον κατασκευαστή. Διατηρείται για συνιστώσες που φιλοξενούνται από τον Ανάδοχο ή εγκαθίστανται on-premises. | Νέα διατύπωση: «Για συνιστώσες παρεχόμενες ως SaaS από τον κατασκευαστή, γίνεται δεκτή η τεκμηρίωση ισοδύναμων ή ισχυρότερων ελέγχων ασφάλειας μέσω της αρχιτεκτονικής της πλατφόρμας και αναγνωρισμένων πιστοποιήσεων (ISO/IEC 27001, SOC 2 Type II, ISO/IEC 27017). Για συνιστώσες φιλοξενούμενες από τον Ανάδοχο ή εγκατεστημένες on-premises, η απαίτηση WAF/UTM παραμένει υποχρεωτική.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 13 | **Ενότητα 2.7 – Α/Α 7 Attack Simulation (σελ. 14)** | Ζητείται διευκρίνιση εάν το Attack Simulation / Purple Teaming είναι μέρος της βασικής υπηρεσίας ή προαιρετικό, και καθορισμός συχνότητας, scope, effort και παραδοτέων. | **ΔΙΕΥΚΡΙΝΙΣΗ – ΥΠΟΧΡΕΩΤΙΚΟ ΜΕ ΟΡΙΟΘΕΤΗΣΗ** | Το αίτημα διευκρίνισης γίνεται δεκτό ως προς την ανάγκη οριοθέτησης. Η υπηρεσία παραμένει υποχρεωτική και μέρος της βασικής προσφοράς, με σαφώς καθορισμένο αντικείμενο ώστε να είναι συγκρίσιμη η κοστολόγηση. | Νέα διατύπωση: «Περιλαμβάνονται στη βασική υπηρεσία δύο (2) ασκήσεις προσομοίωσης επίθεσης ανά έτος, βασισμένες στο πλαίσιο MITRE ATT&CK. Αντικείμενο κάθε άσκησης: κατ' ελάχιστον δεκαπέντε (15) τεχνικές σε τουλάχιστον πέντε (5) τακτικές, εκτελούμενες σε συμφωνημένο δείγμα endpoints και servers. Παραδοτέα: αναφορά αποτελεσμάτων ανά τεχνική (detected / alerted / blocked / missed), ανάλυση κενών ανίχνευσης, σχέδιο αποκατάστασης με χρονοδιάγραμμα και επανέλεγχος των κενών εντός τριάντα (30) ημερών. Η άσκηση εκτελείται σε συνεννόηση με την Αναθέτουσα Αρχή και δεν περιλαμβάνει destructive ενέργειες.» |
| 14 | **Ενότητα 3.1 – Α/Α 11 Dark Web Monitoring (σελ. 15)** | Ζητείται διευκρίνιση εάν είναι υποχρεωτικό ή προαιρετικό και ευθυγράμμιση με την Ενότητα 2.7, όπου αντίστοιχες δυνατότητες αναφέρονται ως optional. | **ΔΙΕΥΚΡΙΝΙΣΗ – ΥΠΟΧΡΕΩΤΙΚΟ ΜΕ ΟΡΙΟΘΕΤΗΣΗ** | Επιβεβαιώνεται η ασυμφωνία μεταξύ των Ενοτήτων 2.7 και 3.1 και αίρεται. Η υπηρεσία παραμένει υποχρεωτική, με καθορισμένο εύρος παρακολούθησης. | Η Ενότητα 2.7 ευθυγραμμίζεται με την Ενότητα 3.1. Νέα διατύπωση: «Το Dark Web Monitoring περιλαμβάνεται στη βασική υπηρεσία και καλύπτει κατ' ελάχιστον: τα εταιρικά domains και υποτομείς, τα εταιρικά domains ηλεκτρονικού ταχυδρομείου, τις εμπορικές ονομασίες και τα σήματα του Οργανισμού, τα εύρη δημόσιων IP διευθύνσεων, καθώς και έως είκοσι (20) ονομαστικά παρακολουθούμενα στελέχη. Παραδοτέα: μηνιαία αναφορά ευρημάτων και άμεση ειδοποίηση (εντός τεσσάρων ωρών από τον εντοπισμό) σε περίπτωση διαρροής διαπιστευτηρίων ή δεδομένων.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 15 | **Ενότητα 3.1 – Α/Α 12 & 13**<br>**DNS Security (σελ. 15)** | Η απαίτηση επιβάλλει dedicated DNS Security λύση και συγκεκριμένη αρχιτεκτονική, αποκλείοντας ισοδύναμη προστασία μέσω NGFW, EDR/XDR, SWG ή NDR. Ζητείται outcome-based απαίτηση. | **ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό. Η απαίτηση αναδιατυπώνεται με βάση το επιδιωκόμενο αποτέλεσμα και όχι τη μορφή υλοποίησης. | Νέα διατύπωση: «Απαιτείται δυνατότητα ασφάλειας DNS που καλύπτει κατ' ελάχιστον: παρεμπόδιση πρόσβασης σε κακόβουλα domains βάσει threat intelligence, ανίχνευση DNS tunneling και αλγορίθμων παραγωγής domain (DGA), ανίχνευση επικοινωνίας command-and-control, πλήρη καταγραφή ερωτημάτων DNS και προώθησή τους στο SIEM για συσχέτιση. Η λειτουργικότητα δύναται να παρέχεται από αποκλειστική λύση DNS Security, από NGFW, SWG, NDR ή EDR/XDR, ή από την υφιστάμενη υποδομή DNS, εφόσον καλύπτεται το σύνολο των ανωτέρω απαιτήσεων.» |
| 16 | **Ενότητα 3.2**<br>**SOC Staffing** | Προτείνεται να καθοριστεί ελάχιστη ομάδα SOC δέκα (10) αναλυτών σε L1/L2/L3, πλέον ρόλων διοίκησης, με υποβολή βιογραφικών του συνόλου της ομάδας. | **ΔΕΝ ΓΙΝΕΤΑΙ ΑΠΟΔΕΚΤΟ** | Το αίτημα δεν γίνεται δεκτό. Ο καθορισμός αυθαίρετου ελάχιστου αριθμού προσωπικού συνιστά καθορισμό του οργανωτικού μοντέλου του παρόχου και όχι απαίτηση αποτελέσματος. Θα απέκλειε παρόχους με διαφορετικά, εξίσου αποτελεσματικά μοντέλα λειτουργίας (αυτοματοποίηση, SOAR, follow-the-sun) και θα ήταν εξίσου περιοριστικός με τα σημεία που ο ίδιος ο προσφέρων επικαλείται. Η Αναθέτουσα Αρχή διασφαλίζει την επιχειρησιακή επάρκεια μέσω μετρήσιμων SLA και τεκμηρίωσης κάλυψης. | Αντ' αυτού προστίθενται οι ακόλουθες απαιτήσεις:<br>• Τεκμηρίωση πραγματικής κάλυψης 24x7x365 (μοντέλο βαρδιών, τοποθεσίες, εφεδρεία, σχέδιο συνέχειας του SOC).<br>• Μετρήσιμα SLA ανά επίπεδο σοβαρότητας: χρόνος ανίχνευσης, χρόνος ειδοποίησης, χρόνος έναρξης ανταπόκρισης, με ρήτρες μη συμμόρφωσης.<br>• Βιογραφικά και πιστοποιήσεις για συγκεκριμένους καίριους ρόλους: SOC Manager, Lead L3 Analyst / Threat Hunter, Incident Response Lead, Service Delivery Manager.<br>• Δήλωση συνολικού μεγέθους ομάδας SOC και αναλογίας αναλυτών ανά εξυπηρετούμενο πελάτη, ως στοιχείο τεκμηρίωσης (βαθμολογούμενο, μη αποκλειστικό).<br>• Υποχρέωση προηγούμενης έγκρισης αντικατάστασης καίριων ρόλων. |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 17 | **Ενότητα 4.1 – Α/Α 1**<br>**On-Premises EDR/XDR (σελ. 19)** | Η απαίτηση η ίδια λύση να υποστηρίζει full on-premises, SaaS και hybrid deployment αποκλείει σύγχρονους cloud-native EDR/XDR κατασκευαστές. Ζητείται αποδοχή secure SaaS πλατφορμών. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό ότι η απαίτηση πλήρους on-premises εγκατάστασης για το σύνολο του περιβάλλοντος είναι δυσανάλογη. Διατηρείται περιορισμένη απαίτηση για τμήματα του περιβάλλοντος με ειδικές ανάγκες απομόνωσης. | Νέα διατύπωση: «Γίνονται δεκτές πλατφόρμες EDR/XDR παρεχόμενες ως SaaS, εφόσον πληρούνται οι απαιτήσεις τοπικότητας δεδομένων εντός ΕΕ/ΕΟΧ, απομόνωσης tenant και διαχείρισης κλειδιών της Ενότητας Α – Α/Α 4. Απαιτείται επιπλέον δυνατότητα λειτουργίας των agents σε συστήματα χωρίς άμεση πρόσβαση στο διαδίκτυο, μέσω proxy, relay ή ισοδύναμου μηχανισμού, καθώς και διατήρηση βασικών δυνατοτήτων προστασίας σε κατάσταση εκτός σύνδεσης (offline protection).» |
| 18 | **Ενότητα 4.1 – Α/Α 8**<br>**Software Compatibility (σελ. 19)** | Απόλυτη απαίτηση συμβατότητας με οποιοδήποτε μη καθορισμένο λογισμικό χωρίς bluescreens ή process crashes δεν είναι αντικειμενικά μετρήσιμη. Ζητείται αντικατάσταση με vendor-supported compatibility και pilot testing. | **ΑΠΟΔΕΚΤΟ – ΜΕ ΕΝΙΣΧΥΜΕΝΗ ΔΙΑΤΥΠΩΣΗ** | Γίνεται δεκτό ότι η υφιστάμενη διατύπωση δεν είναι αντικειμενικά μετρήσιμη. Αντικαθίσταται με απαιτήσεις ελεγχόμενης διανομής ενημερώσεων, οι οποίες αντιμετωπίζουν ουσιαστικότερα τον υποκείμενο κίνδυνο και ευθυγραμμίζονται με τις υποχρεώσεις της Αναθέτουσας Αρχής για διαχείριση κινδύνου τρίτων παρόχων ΤΠΕ κατά DORA. | Νέα διατύπωση: «Απαιτείται:<br>(α) τεκμηριωμένη συμβατότητα υποστηριζόμενη από τον κατασκευαστή για το σύνολο των λειτουργικών συστημάτων και των κρίσιμων εφαρμογών της Αναθέτουσας Αρχής, όπως θα οριστικοποιηθούν κατά τη φάση σχεδιασμού,<br>(β) δοκιμαστική εγκατάσταση (pilot) σε αντιπροσωπευτικό δείγμα πριν από την καθολική εγκατάσταση,<br>(γ) σταδιακή/κλιμακωτή διανομή ενημερώσεων agent και content (ring-based deployment) με ομάδα ελέγχου (canary), υπό τον έλεγχο και το χρονοδιάγραμμα της Αναθέτουσας Αρχής,<br>(δ) δυνατότητα άμεσης αναστροφής (rollback) ενημέρωσης,<br>(ε) συμβατική ευθύνη του Αναδόχου για διακοπή λειτουργίας συστημάτων προκληθείσα από ενημέρωση agent ή content.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 19 | **Ενότητα 4.3 – Α/Α 19**<br>**Ransomware Rollback (σελ. 21)** | Το native ransomware rollback δεν υποστηρίζεται από αρκετούς μεγάλους κατασκευαστές και αποτελεί συγκεκριμένη προσέγγιση υλοποίησης. Ζητείται αντικατάσταση με outcome-based απαίτηση. | **ΜΕΡΙΚΩΣ ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτή η αφαίρεση από τις υποχρεωτικές απαιτήσεις. Η δυνατότητα δεν διαγράφεται αλλά μετατρέπεται σε βαθμολογούμενη, καθώς προσφέρει ουσιαστικό πλεονέκτημα όπου υπάρχει. | ΥΠΟΧΡΕΩΤΙΚΑ: πρόληψη, ανίχνευση συμπεριφοράς κρυπτογράφησης, αυτόματη απομόνωση τερματικού (host isolation), τερματισμό κακόβουλων διεργασιών, ανάλυση αιτίου (root cause) και υποστήριξη αποκατάστασης.<br>ΒΑΘΜΟΛΟΓΟΥΜΕΝΟ (μη αποκλειστικό): native ransomware rollback / αυτόματη επαναφορά αρχείων, με δήλωση περιορισμών (τύποι αρχείων, χρονικό παράθυρο, απαιτήσεις αποθηκευτικού χώρου). |
| 20 | **Ενότητα 4.3 – Α/Α 22**<br>**Virtual Patching (σελ. 22)** | Ο μηχανισμός transaction-level virtual patching αποτελεί IPS/NGFW/WAF δυνατότητα και όχι τυπική EDR/XDR λειτουργία. Ζητείται αφαίρεση ή αποδοχή ισοδύναμων τεχνολογιών. | **ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό. Η απαίτηση αναδιατυπώνεται ώστε να περιγράφει το επιδιωκόμενο αποτέλεσμα και όχι τον συγκεκριμένο μηχανισμό. | Νέα διατύπωση: «Απαιτείται δυνατότητα αποτροπής εκμετάλλευσης γνωστών και άγνωστων ευπαθειών σε επίπεδο τερματικού, μέσω exploit prevention, προστασίας μνήμης, αποτροπής κλιμάκωσης δικαιωμάτων και συμπεριφορικού αποκλεισμού. Γίνονται δεκτοί ισοδύναμοι μηχανισμοί, περιλαμβανομένου του virtual patching, εφόσον τεκμηριώνεται η κάλυψη γνωστών CVE και η αποτελεσματικότητα σε ανεξάρτητες δοκιμές.» |
| 21 | **Ενότητα 4.4 – Α/Α 5**<br>**EDR/XDR Log Retention (σελ. 22)** | Ζητείται διευκρίνιση εάν οι 12 μήνες αφορούν alerts/incidents, audit logs ή full raw telemetry. Προτείνονται 3 μήνες searchable telemetry και 9 μήνες μέσω SIEM/archive. | **ΔΙΕΥΚΡΙΝΙΣΗ – ΑΠΟΔΕΚΤΟ** | Η ασάφεια αναγνωρίζεται και αίρεται. Η πρόταση του προσφέροντος γίνεται δεκτή, με διακριτό ορισμό ανά κατηγορία δεδομένων. | Νέα διατύπωση: «Οι απαιτήσεις διατήρησης διαφοροποιούνται ως εξής:<br>• Alerts, incidents, detections και audit/administrative logs: δώδεκα (12) μήνες, αναζητήσιμα, δυνάμενα να τηρούνται στο SIEM ή σε αρχείο.<br>• Raw endpoint telemetry: ενενήντα (90) ημέρες πλήρως αναζητήσιμα στην κονσόλα EDR/XDR, με δυνατότητα προώθησης επιλεγμένων κατηγοριών στο SIEM.<br>• Ο προσφέρων δηλώνει ρητά τυχόν επιπτώσεις σε αδειοδότηση ή αποθηκευτικό χώρο.» |

| Α/Α | Σημείο RFP | Σχόλιο προσφέροντος (σύνοψη) | Απόφαση | Απάντηση ΚΕΔΙΠΕΣ | Νέα διατύπωση / Ενέργεια |
|---|---|---|---|---|---|
| 22 | **Ενότητα 4.4 – Α/Α 10 Automated Patching (σελ. 23)** | Το automated OS και third-party patch deployment αποτελεί Patch Management λειτουργικότητα και όχι core EDR/XDR δυνατότητα. Ζητείται αφαίρεση ή μετατροπή σε optional· να αρκούν vulnerability visibility και risk prioritization. | **ΑΠΟΔΕΚΤΟ** | Γίνεται δεκτό. Η αυτοματοποιημένη εγκατάσταση διορθώσεων αφαιρείται από το υποχρεωτικό αντικείμενο EDR/XDR. | ΥΠΟΧΡΕΩΤΙΚΑ: εντοπισμός και απογραφή ευπαθειών σε επίπεδο τερματικού, συσχέτιση με CVE και CVSS, ιεράρχηση βάσει κινδύνου και πραγματικής εκμεταλλευσιμότητας, περιοδική αναφορά και παρακολούθηση εξέλιξης.<br>ΠΡΟΑΙΡΕΤΙΚΑ (χωριστή τιμολόγηση): αυτοματοποιημένη εγκατάσταση διορθώσεων λειτουργικού συστήματος και λογισμικού τρίτων. |
| 23 | **Στοιχεία Sizing / Παρακολουθούμενα Συστήματα** | Ζητείται ο συνολικός αριθμός και τύπος των συστημάτων που θα παρακολουθούνται (endpoints, servers ανά ρόλο, security/networking assets, λοιπές υποδομές και cloud υπηρεσίες), για ορθό sizing και συγκρίσιμη κοστολόγηση. | **ΑΠΟΔΕΚΤΟ – ΜΕ ΕΛΕΓΧΟΜΕΝΗ ΔΙΑΘΕΣΗ** | Το αίτημα είναι βάσιμο και αναγκαίο για τη συγκρισιμότητα των προσφορών. Δεδομένου ωστόσο ότι πρόκειται για λεπτομερή αποτύπωση της υποδομής ασφάλειας της Αναθέτουσας Αρχής, τα στοιχεία δεν δημοσιεύονται σε ανοικτή μορφή. | Ενέργειες Αναθέτουσας Αρχής:<br>(α) Δημοσιεύεται συνοπτικός πίνακας sizing με εύρη ανά κατηγορία (endpoints ανά λειτουργικό σύστημα, servers ανά ρόλο, δικτυακές και συσκευές ασφάλειας ανά τύπο, cloud tenants, αριθμός χρηστών και τοποθεσιών).<br>(β) Δημοσιεύεται μέσο και αιχμιακό μέγεθος καταγραφών (EPS και GB ημερησίως), το οποίο αποτελεί το κρίσιμο μέγεθος κοστολόγησης.<br>(γ) Αναλυτικός κατάλογος συστημάτων διατίθεται σε εγγεγραμμένους ενδιαφερόμενους κατόπιν υπογραφής συμφωνίας εμπιστευτικότητας.<br>(δ) Διευκρινίζεται ρητά το εύρος ως προς τυχόν συστήματα που αφορούν τον Οργανισμό Χρηματοδοτήσεως Στέγης και τους εξωτερικούς διαχειριστές.<br>(ε) Λόγω της ουσιώδους φύσης της συμπλήρωσης, εξετάζεται παράταση της προθεσμίας υποβολής προσφορών. |

## 6. Τελικές παρατηρήσεις

Οι προσφέροντες οφείλουν να λάβουν υπόψη το παρόν έγγραφο κατά τη σύνταξη των προσφορών τους. Σε περίπτωση απόκλισης μεταξύ του αρχικού Παραρτήματος 2 και του παρόντος, υπερισχύει το παρόν.

Τυχόν περαιτέρω αιτήματα διευκρινίσεων υποβάλλονται εγγράφως, εντός της προθεσμίας που ορίζεται στα έγγραφα του διαγωνισμού, και απαντώνται με τον ίδιο τρόπο προς όλους τους ενδιαφερόμενους οικονομικούς φορείς.

Σημειώνεται ότι στο υποβληθέν έγγραφο σχολίων εντοπίστηκαν επαναλαμβανόμενες και ελλιπείς αριθμήσεις. Για λόγους σαφήνειας, η αρίθμηση του παρόντος πίνακα είναι αυτοτελής και αποτελεί τη μοναδική αναφορά για κάθε περαιτέρω αλληλογραφία επί των συγκεκριμένων σημείων.