ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΤΕΧΝΟΛΟΓΙΑΣ
ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΜΕΣΩΝ
ΔΙΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΛΛΗΝΙΚΗ ΡΑΔΙΟΦΩΝΙΑ ΤΗΛΕΟΡΑΣΗ Α.Ε.

DAMIANOS MANIATAKOS
29/09/2025 12:04

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ
ΥΠΗΡΕΣΙΕΣ S.O.C. για τρία (3) έτη

ΠΑΝΤΑΖΗΣ ΣΩΤΗΡΙΟΣ

Περιεχόμενα

1 Φυσικό αντικείμενο

Το παρόν έργο αφορά την προμήθεια υπηρεσιών Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων (Security Operations Center - Managed Security Services, SOC MSS), με συνεχή λειτουργία 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα (24x7), για χρονικό διάστημα τριών (3) ετών.

Σκοπός του έργου είναι η παρακολούθηση, ανάλυση και αντιμετώπιση περιστατικών ασφάλειας που σχετίζονται με τα πληροφοριακά συστήματα της ΕΡΤ Α.Ε., με στόχο την ενίσχυση της κυβερνοασφάλειας και την προστασία των ψηφιακών υποδομών του Οργανισμού.

1.1 Υπάρχουσα Υποδομή Ασφάλειας

Ο αριθμός των χρηστών της ΕΡΤ Α.Ε. που δύνανται να είναι ταυτόχρονα συνδεδεμένοι στο διαδίκτυο ανέρχεται σε 2000. Για την δικτυακή ασφάλεια, η ΕΡΤ Α.Ε. χρησιμοποιεί τέσσερα συστήματα ασφαλείας τύπου firewall από διαφορετικούς κατασκευαστές. Το λογισμικό αυτών των συστημάτων παρέχει πέντε κύριες υπηρεσίες: firewall, VPN, identity awareness, advanced networking και quality of service, καθώς και τρεις υπηρεσίες Next Generation Firewall (IPS & application control, URL filtering). Επιπλέον λειτουργεί υπηρεσία φιλτραρίσματος DNS (Umbrella Security). Όλοι οι σταθμοί εργασίας και οι διακομιστές διαθέτουν προστασία με χρήση λύσης EDR (Endpoint Detection and Response). Στην πλατφόρμα ηλεκτρονικού ταχυδρομείου της ΕΡΤ Α.Ε. λειτουργούν υπηρεσίες για την ασφάλεια αλληλογραφίας. Οι web εφαρμογές εξυπηρετούνται μέσω WAF (Web application Firewall).

1.2 Ζητούμενες υπηρεσίες

Η ΕΡΤ Α.Ε. επιθυμεί τη συνεχή παρακολούθηση της υποδομής της σε σχέση με το επίπεδο ασφαλείας, την αντιμετώπιση απειλών, την ανάλυση των περιστατικών και την άμεση ενημέρωση για πιθανά συμβάντα ασφαλείας που σχετίζονται με αυτήν σε 24ωρη βάση. Για το λόγο αυτό ο Ανάδοχος θα πρέπει να παρέχει υπηρεσία παρακολούθησης και διαχείρισης περιστατικών ασφαλείας σε πραγματικό χρόνο 24x7. Οι προσφερόμενες υπηρεσίες θα πρέπει να περιλαμβάνουν κατ΄ελάχιστο:

- **Υπηρεσία SOC**: Ο Ανάδοχος θα παρακολουθεί την υποδομή που είναι εντός του πλαισίου της εν λόγω υπηρεσίας και σε περίπτωση

περιστατικού ασφαλείας θα πραγματοποιεί τις ενδεδειγμένες ενέργειες περιορισμού και αντιμετώπισης και θα ενημερώνει την ΕΡΤ Α.Ε. σύμφωνα με το συμφωνημένο επίπεδο υπηρεσιών (Service Level Agreement).

- **Αυτοματοποιημένη Υπηρεσία Διερεύνησης Περιστατικών Ασφαλείας**: Ο Ανάδοχος θα πρέπει να παρέχει υπηρεσία αυτοματοποιημένης διερεύνησης περιστατικών ασφαλείας με σκοπό την επιτάχυνση της ανάλυσης και την παροχή προτάσεων μετριασμού. Η υπηρεσία δύναται να βασίζεται σε τεχνολογίες αυτοματισμού, τεχνητής νοημοσύνης ή/και έτοιμες ροές εργασίας (SOAR), με στόχο τη συστηματική αξιολόγηση του συμβάντος και την παροχή ενεργειών απόκρισης
- **Υπηρεσία Ανίχνευσης και Απόκρισης (Managed Detection and Response):** Σε περίπτωση ανίχνευσης ενός περιστατικού ο Ανάδοχος θα πρέπει να παρέχει υπηρεσία απόκρισης με σκοπό την καταστολή της επίθεσης.
- **Υπηρεσία ενορχήστρωσης και αυτοματισμού**: Ο Ανάδοχος για την άμεση και αποτελεσματική αντιμετώπιση κυβερνοεπιθέσεων, θα πρέπει να παρέχει τις κατάλληλες ροές εργασιών (workflows) και οδηγιών εργασίας (playbooks).
- **Υπηρεσία Cybersecurity Threat Intelligence**: Ο Ανάδοχος θα πρέπει να παρέχει έγκαιρη ενημέρωση για πιθανές απειλές, ευπάθειες και διαρροές που σχετίζονται με τα πληροφοριακά Assets της ΕΡΤ Α.Ε., μέσω Υπηρεσίας **Cyber Threat Intelligence** ή αντίστοιχης.
- **Υπηρεσία EDR**: Ο Ανάδοχος θα πρέπει να παράσχει στην ΕΡΤ Α.Ε. τις απαιτούμενες άδειες χρήσης λύσης EDR, να τις εγκαταστήσει στα τερματικά, να πραγματοποιήσει migration των υφιστάμενων κανόνων και εξαιρέσεων και να εκπαιδεύσει το αρμόδιο προσωπικό της ΕΡΤ Α.Ε. στη λειτουργία της λύσης εντός 2 μηνών από την έναρξη του έργου. Η προσφερόμενη EDR λύση θα πρέπει να περιλαμβάνεται στους leaders του Gartner Magic Quadrant για Endpoint Protection Platforms. Η προσφερόμενη λύση θα πρέπει να λειτουργεί μέσω Cloud.

Η ΕΡΤ Α.Ε. θα πρέπει να μπορεί να παρακολουθεί σε πραγματικό χρόνο τα εν λόγω περιστατικά μέσω κατάλληλης Δικτυακής Πύλης, καθώς και να έχει πλήρη πρόσβαση σε όλα τα αρχεία καταγραφής συμβάντων. Επίσης θα πρέπει να ενημερώνεται για πιθανά περιστατικά ασφαλείας σε 24ωρη βάση μέσω e-mail, sms ή τηλεφωνικής κλήσης, ανάλογα με την κρισιμότητά τους. Ο υποψήφιος ανάδοχος οφείλει να περιγράψει τη μεθοδολογία διαβάθμισης των

περιστατικών ασφάλειας. Ειδικότερα, για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται ως ύψιστης κρισιμότητας απαιτείται τηλεφωνική ενημέρωση της ΕΡΤ Α.Ε. εντός 10 λεπτών από τη στιγμή εκδήλωσης του περιστατικού. Η συλλογή και επεξεργασία των σχετικών πληροφοριών θα γίνεται σε κατάλληλη SOC υποδομή του αναδόχου από μηχανικούς που διαθέτουν κατάλληλες πιστοποιήσεις ασφάλειας. Ο ανάδοχος, πλην της άμεσης επέμβασης και ενημέρωσης για τυχόν συμβάντα ασφαλείας, οφείλει να παραδίδει και την σχετική αναφορά σε μηνιαία βάση.

2 Τεχνική Περιγραφή ζητούμενης υπηρεσίας SOC

Στο πλαίσιο της υπηρεσίας αυτής ο Ανάδοχος:

- Θα συντάξει τη μεθοδολογία διαβάθμισης των περιστατικών ασφάλειας και ενημέρωσης της ΕΡΤ Α.Ε. ανάλογα με την κρισιμότητα των εν λόγω περιστατικών. Για παράδειγμα, ένα περιστατικό ασφαλείας είναι η αδυναμία δικτυακής πρόσβασης λόγω συγκεκριμένης επίθεσης. Το περιστατικό αυτό μπορεί να διαβαθμιστεί ως προς τη σοβαρότητά του ανάλογα του πιθανού χρόνου απουσίας πρόσβασης και της ιδιαιτερότητας της υποδομής (πχ κεντρικός-περιφερειακός router).
- Θα συλλέγει σε πραγματικό χρόνο τα αρχεία καταγραφών ασφαλείας (security logs) της υποδομής της ΕΡΤ Α.Ε., τα οποία είναι εντός του πεδίου εφαρμογής των εν λόγω υπηρεσιών.
- Θα επεξεργάζεται τα συλλεχθέντα αρχεία καταγραφών, θα τα αναλύει άμεσα μέσω ευφυών αλγορίθμων συσχέτισης με γνωστά δεδομένα επιθέσεων, για τον εντοπισμό ύποπτων ενεργειών, μη φυσιολογικής κίνησης και/ή περιστατικών ασφαλείας και θα αποκρίνεται επίσης άμεσα στην περίπτωση εντοπισμού κάποιου περιστατικού, σύμφωνα με την υιοθετημένη πολιτική αντιμετώπισης κρίσεων και περιστατικών ασφαλείας.
- Θα παρέχει συνεχή υποστήριξη στην ΕΡΤ Α.Ε. κατά τη διάρκεια ενός περιστατικού ασφάλειας, ώστε να πραγματοποιηθούν ομαλά όλες οι ενέργειες που προβλέπονται στην υιοθετημένη πολιτική αντιμετώπισης κρίσεων και περιστατικών ασφάλειας. Εφόσον το περιστατικό είναι κρίσιμο θα παρέχει και παρουσία κατάλληλου πιστοποιημένου προσωπικού στα HQ της ΕΡΤ Α.Ε..
- Θα ενημερώνει την ΕΡΤ Α.Ε. για πιθανά περιστατικά ασφάλειας σε 24ωρη βάση μέσω e-mail και sms ή τηλεφωνικής κλήσης ανάλογα με

την κρισιμότητά τους. Ειδικότερα για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται ύψιστης κρισιμότητας και μπορεί να επιφέρουν ιδιαίτερα σημαντικές επιπτώσεις στις υποδομές της ΕΡΤ Α.Ε., απαιτείται τηλεφωνική ενημέρωση εντός 10 λεπτών από τη στιγμή εκδήλωσης του περιστατικού.

- Θα εκπαιδεύσει το Φορέα στη χρήση του portal με πρόγραμμα εκπαίδευσης που θα υποβάλλει στην προσφορά του. Το πρόγραμμα εκπαίδευσης θα είναι διάρκειας 10 ωρών σε 2 group μηχανικών πληροφορικής της ΕΡΤ Α.Ε. (2 group των 10 ωρών έκαστο)
- Για κάθε περιστατικό ασφάλειας που θα διαπιστωθεί:
  - θα υποστηρίξει άμεσα την ΕΡΤ Α.Ε. στην αντιμετώπιση του.
  - θα αναλύσει τα αίτια δημιουργίας και θα προτείνει μέτρα αντιμετώπισης, τα οποία θα αξιοποιηθούν για την κατάλληλη βελτίωση.
  - θα καταγράψει και θα αναφέρει στην ΕΡΤ Α.Ε. το ιστορικό δημιουργίας και αντιμετώπισης του συμβάντος.
- Για την παρακολούθηση της ασφάλειας της ΕΡΤ Α.Ε., ο Ανάδοχος θα ακολουθήσει μια δομημένη προσέγγιση υλοποίησης, συμμορφωμένη με διεθνή πρότυπα και βέλτιστες πρακτικές και υποστηριζόμενη από κατάλληλα εργαλεία και μηχανισμούς ΤΠΕ, ώστε να ανταπεξέλθει ικανοποιητικά στις προαναφερθείσες απαιτήσεις ελέγχου ασφάλειας αλλά και στην επίτευξη των στόχων του έργου. Ειδικότερα, θα κάνει χρήση Συστήματος Διαχείρισης Πληροφοριών και Περιστατικών Ασφάλειας ως υπηρεσία (Security Information and Event Management System as a Service -SIEM as a Service-)
- Μηνιαία, ο Ανάδοχος θα παρουσιάζει στην ΕΡΤ Α.Ε. τις ενέργειες που πραγματοποίησε, τα πορίσματα από τις ενέργειες παρακολούθησης καθώς και τις βελτιωτικές προτάσεις που πρέπει να πραγματοποιηθούν στο πλαίσιο αναβάθμισης του επιπέδου ασφάλειας του Δικτύου.

Ο Ανάδοχος οφείλει να εκπαιδεύσει θα πρέπει να εκπαδεύσει αρμόδιο προσωπικό της ΕΡΤ Α.Ε. και στην λειτουργία την προσφερόμενης λύσης EDR (2 group 10 ωρών έκαστο)

Στη συνέχεια ακολουθεί Asset List των συστημάτων που θα πρέπει να ενταχθούν στην υπηρεσία (log sources) κατ' ελάχιστον. Μελλοντικές προσθήκες συστημάτων οι οποίες θα πραγματοποιηθούν στο χρονικό διάστημα μέχρι την υπογραφή της σύμβασης ή και κατά τη διάρκεια αυτής, θα πρέπει να εντάσσονται στις υπηρεσίες

παρακολούθησης χωρίς διαφοροποίηση του κόστους ή της ποιότητας των υπηρεσιών αυτής.

Τύπος Συστήματος	Ποσότητα
Enterprise FW appliances	12
SMB FW appliances	19
Hypervisors	15
Physical Servers (windows + Linux)	50
Virtual Windows Servers	150
Virtual Linux Servers	150
Storage Devices	10
Network Switches	150
Network Routers	8
Wireless Controllers (200 APs)	6
EDR management (2200 endpoints)	1
Office 365 (2800 mailboxes)	1
Mail security (2800 mailboxes)	1
DNS filtering (CISCO Umbrella)	1
MFA platform (600 users)	1
PAM solution (100 users)	1

3 Πίνακες Συμμόρφωσης

Πίνακας-1. Αναλυτικές λειτουργικές προδιαγραφές Υπηρεσιών Επιχειρησιακού Κέντρου Ασφάλειας - Παρακολούθησης και Διαχείρισης Περιστατικών Ασφάλειας

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία Επιχειρησιακές Κέντρου Ασφάλειας (SOC as a Service)				
1.1	Ο υποψήφιος Ανάδοχος θα πρέπει να διαθέτει Κέντρο Επιχειρησιακής Ασφάλειας (SOC) εντός της ΕΕ, με	**ΝΑΙ**		

	αποδεδειγμένη δυνατότητα συνεχούς λειτουργίας (24x7) και επιχειρησιακής συνέχειας (Business Continuity) μέσω εναλλακτικού χώρου ή εφεδρικής δομής. Να περιγραφεί αναλυτικά η αρχιτεκτονική, οι διαδικασίες και τα μέσα που χρησιμοποιούνται για την εξασφάλιση της επιχειρησιακής συνέχειας του SOC.			
1.2	Παρακολούθηση, ανάλυση και αξιολόγηση των περιστατικών ασφαλείας σε πραγματικό χρόνο 24x7 .	**ΝΑΙ**		
1.3	Το SOC να διαθέτει ικανό αριθμό αναλυτές επιπέδου 1, επιπέδου 2 και επιπέδου 3	**ΝΑΙ**		
1.4	Οι αναλυτές SOC tier 1 είναι υπεύθυνοι για την παρακολούθηση και τη διαλογή ειδοποιήσεων (Triage) σε πραγματικό χρόνο. Οι αναλυτές SOC tier 2 λειτουργούν ως σημείο κλιμάκωσης για τους αναλυτές tier 1 κατά τη διάρκεια της ανάλυσης και της απόκρισης συμβάντων.	**ΝΑΙ**		
1.5	Οι αναλυτές SOC Tier 2 θα πρέπει να είναι σε θέση να παρέχουν Incident response, (coordinate investigation, containment), threat hunting, big data analysis και ετοιμασία εκθέσεων προς την Αναθέτουσα Αρχή.	**ΝΑΙ**		
1.6	Οι αναλυτές SOC Tier 3 θα είναι αρμόδιοι για τα παρακάτω: 1. **Αρχιτεκτονική και Σχεδιασμός Απόκρισης σε Περιστατικά (IR Architecture & Playbooks)** • Σχεδιασμός και βελτιστοποίηση διαδικασιών IR. • Ανάπτυξη και επικαιροποίηση playbooks για Tier 1 και Tier 2. • Συντονισμός με εξωτερικούς φορείς			

	(CERTs, law enforcement). 2. **Advanced Threat Hunting & Behavioral Analytics** • Ανάλυση σύνθετων απειλών (APT, zero-day). • Χρήση machine learning και UEBA (User and Entity Behavior Analytics). • Ανίχνευση lateral movement και persistence mechanisms. 3. **Digital Forensics & Malware Reverse Engineering** • Ανάλυση μνήμης, δίσκων, δικτύου και αρχείων καταγραφής. • Αντίστροφη μηχανική κακόβουλου λογισμικού για αναγνώριση TTPs (Tactics, Techniques, Procedures). 4. **Threat Intelligence & Attribution** • Ανάλυση και συσχέτιση δεδομένων για αναγνώριση επιτιθέμενων ομάδων. • Παρακολούθηση dark web και πληροφοριών OSINT. • Σύνθεση αναφορών στρατηγικού επιπέδου για τη διοίκηση της Διεύθυνσης			

	Πληροφορικής της EPT A.E. 5. **Συμμετοχή σε Red/Blue/Purple Team Exercises** • Συνεργασία με ομάδες Red για αξιολόγηση αμυντικών μηχανισμών. • Ανάλυση ευρημάτων και ενσωμάτωση lessons learned. 6. **Στρατηγική Αναφορά και Ενημέρωση Διοίκησης** • Παροχή αναλύσεων κινδύνου και προτάσεων πολιτικής ασφάλειας.			
1.7	Ο Ανάδοχος θα πρέπει να διατηρεί ένα ενημερωμένο Σχέδιο Συνέχειας Επιχειρήσεων (BCP/DRP) σε περίπτωση που για λόγους ανωτέρας βίας δεν είναι διαθέσιμο το SOC του.	**ΝΑΙ**		
1.8	Η EPT A.E. θα πρέπει να έχει πρόσβαση σε πίνακες εργαλείων εποπτείας και αναφορών (πχ dashboards) μέσω κατάλληλης διεπαφής, οι οποίοι θα παρέχουν πληροφορίες για την κατάσταση ασφάλειας, τις τρέχουσες απειλές και την πορεία διερεύνησης περιστατικών. Οι πίνακες αυτοί θα πρέπει να παρέχουν πλήρη πληροφορία όσον αφορά στα ενεργά περιστατικά, τις κρίσιμες ειδοποιήσεις και τις ενέργειες που έχουν ληφθεί.	**ΝΑΙ**		
1.9	Ενημέρωση για πιθανά περιστατικά ασφαλείας μέσω: • Τηλεφωνικής κλήσης, • E-mail, • SMS, • Collaboration software π.χ. Microsoft	**ΝΑΙ**		

	Teams • Web Portal.			
1.10	Δυνατότητα δημιουργίας εξατομικευμένων κανόνων συσχετισμού σύμφωνα με τις απαιτήσεις και τις ιδιαιτερότητες των πληροφοριακών συστημάτων του Φορέα.	**ΝΑΙ**		
1.11	Δημιουργία περιπτώσεων χρήσης (use cases) βάσει των οποίων θα εντοπίζονται τα περιστατικά ασφαλείας. Περιγράψτε λεπτομερώς τις περιπτώσεις χρήσης Analytics (Analytics Use Cases) που θα είναι διαθέσιμες από την 1η ημέρα της παρακολούθησης.	**ΝΑΙ**		
1.12	Για κάθε περιστατικό θα πρέπει τουλάχιστον να αναφέρεται η ώρα και ημερομηνία, η κρισιμότητα, οι ενέργειες εξάλειψης.	**ΝΑΙ**		
1.13	Τα περιστατικά θα πρέπει να κατηγοριοποιούνται με βάση την κρισιμότητα τους ως ελάχιστο οι ακόλουθες κατηγορίες πρέπει να υπάρχουν Χαμηλή, Μέτρια, Υψηλή. Για κάθε περιστατικό θα πρέπει να αναφέρεται η κατά Mitre ATT&CK Tactics – Techniques and Sub-Technique mapping αντιστοίχιση.	**ΝΑΙ**		
1.14	Εντοπισμός ανωμαλιών (anomaly detection).	**ΝΑΙ**		
1.15	Διαρκής ενημέρωση για νέες απειλές σε παγκόσμιο επίπεδο μέσω Intelligence Feeds.	**ΝΑΙ**		
1.16	Δυνατότητα πρόσβασης σε Web portal το οποίο θα λειτουργεί 24x7, για την παρακολούθηση των περιστατικών και την περαιτέρω διερεύνηση των περιστατικών.	**ΝΑΙ**		
1.17	Δυνατότητα δημιουργίας εξατομικευμένων αναφορών, ανάλογα με τις ανάγκες του Φορέα.	**ΝΑΙ**		
1.18	Δυνατότητα δημιουργίας	**ΝΑΙ**		

	συγκεντρωτικής αναφοράς συμβάντων σε μηνιαία βάση.			
1.19	Κρυπτογράφηση των ηλεκτρονικών πληροφοριών.	**ΝΑΙ**		
1.20	Να παρέχεται υπηρεσία User Behavior Analysis. Να περιγραφεί αναλυτικά.	**ΝΑΙ**		
1.21	Να παρέχεται υπηρεσία ticketing. Να γίνει αποτύπωση λεπτομερώς της προσφερόμενη λύση ticketing / ροής εργασίας για την κλιμάκωση των περιστατικών.	**ΝΑΙ**		
1.22	Η υπηρεσία να υποστηρίζεται από Εγγυημένο Επίπεδο Υπηρεσιών. Να περιγραφεί αναλυτικά. Κατ' ελάχιστο οι απαιτήσεις του χρόνου ενημέρωσης σύμφωνα με κάθε σοβαρότητα Συμβάντος: 1) Ανώτατο επίπεδο κρισιμότητας Μέγιστος χρόνος ενημέρωσης SLA 90 λεπτά . 2) Μέγιστος χρόνος ενημέρωσης SLA μεσαίου επιπέδου κρισιμότητας 4 ώρες 3) Χαμηλότερο επίπεδο κρισιμότητας μέγιστος χρόνος ενημέρωσης SLA 12 ώρες.	**ΝΑΙ**		
1.23	Να προσφερθεί υπηρεσία Forensics. Να περιγραφεί αναλυτικά.	**ΝΑΙ**		
1.24	Να προσφερθούν συμβουλευτικές υπηρεσίες ασφάλειας σχετικά με απειλές, τεχνολογίες ανίχνευσης περιστατικών ασφαλείας, πλάνο απόκρισης κ.λπ.	**ΝΑΙ**		
1.25	Η υπηρεσία θα πρέπει να επιτρέπει την επιλογή διαφορετικών επαφών κλιμάκωσης με βάση τον τύπο και τη σοβαρότητα της ειδοποίησης. Αυτές οι επαφές θα πρέπει να περιλαμβάνουν τον αριθμό τηλεφώνου τους ως προϋπόθεση για το χειρισμό υψηλού προφίλ και κρίσιμων συμβάντων.	**ΝΑΙ**		
1.26	Ο υποψήφιος Ανάδοχος θα πρέπει να παρέχει υπηρεσία Managed Detection and response με την προσφερόμενη	**ΝΑΙ**		

	λύση EDR . Να περιγραφεί αναλυτικά.			
1.27	Πλήρης συμμόρφωση με τα όσα αναφέρονται στις παραγράφους 1.1, 1.2, και 2.			
1.28	Ο υποψήφιος ανάδοχος δεσμεύεται για τα όσα αναγράφονται στην παράγραφο 4 του παρόντος παραρτήματος τεχνικών προδιαγραφών «SLA/MSS SOC».	**ΝΑΙ**		
1.29	Ο υποψήφιος ανάδοχος δεσμεύεται για τα όσα αναγράφονται στην παράγραφο 5 του παρόντος παραρτήματος τεχνικών προδιαγραφών «Λοιπά στοιχεία έργου».	**ΝΑΙ**		
1.30	Ο υποψήφιος ανάδοχος δεσμεύεται για τα όσα αναγράφονται στην παράγραφο 6 του παρόντος παραρτήματος τεχνικών προδιαγραφών «Χρονοδιαγράμματα».	**ΝΑΙ**		

Πίνακας-2. Αναλυτικές λειτουργικές προδιαγραφές Λογισμικού Διαχείρισης Περιστατικών Ασφαλείας (Security Information Event Management)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία SIEM				
2.1	Να προσφερθεί σύστημα SIEM ως υπηρεσία για την συλλογή των αρχείων καταγραφής (logs) που δημιουργούνται από τις πληροφοριακές υποδομές του Φορέα.	ΝΑΙ		
2.2	Ρυθμός συλλογής δεδομένων καταγραφής από τα υπό παρακολούθηση συστήματα.	≥ 2.500 Events per Second		
2.3	Ο υποψήφιος ανάδοχος θα πρέπει να συλλέγει δεδομένα από όλα τα συστήματα που θα υποδείξει η ΕΡΤ Α.Ε. και αποτυπώνονται στην παράγραφο *2 Τεχνική περιγραφή ζητούμενης υπηρεσίας SOC* κατ' ελάχιστον. Μελλοντικές προσθήκες συστημάτων οι οποίες θα πραγματοποιηθούν στο χρονικό	ΝΑΙ		

	διάστημα μέχρι την υπογραφή της σύμβασης ή και κατά τη διάρκεια αυτής, θα πρέπει να εντάσσονται στις υπηρεσίες παρακολούθησης χωρίς διαφοροποίηση του κόστους ή της ποιότητας των υπηρεσιών αυτής.			
2.4	Το λογισμικό της λύσης να είναι στους leaders του Gartner Magic Quadrant τα τελευταία 3 έτη.	ΝΑΙ		
2.5	Η προσφερόμενη λύση θα πρέπει να εγκαθίσταται σε εξειδικευμένες υποδομές με τρόπο που διασφαλίζει την απόδοση, τη διαθεσιμότητα και την ασφάλεια του συστήματος. Οι υποδομές αυτές μπορεί να είναι φυσικές συσκευές (hardware appliances), εικονικές (virtual appliances) ή συνδυασμός αυτών, ανάλογα με τις τεχνικές απαιτήσεις κάθε ρόλου και τη συνολική αρχιτεκτονική της λύσης. Σε περίπτωση όπου οι εικονικές συσκευές (VMs) φιλοξενούνται σε υποδομές του Φορέα, ο Ανάδοχος υποχρεούται να καταθέσει αναλυτικά τις απαιτούμενες προδιαγραφές.	ΝΑΙ		
2.6	Σε περίπτωση που ο Ανάδοχος προσφέρει ιδεατές συσκευές για την κάλυψη κάποιων λειτουργιών, να υποστηρίζονται κατ' ελάχιστο οι Hypervisor Hyper-V και VMWare	ΝΑΙ		
2.7	Η υπηρεσία θα πρέπει καλύπτει κατ' ελάχιστον την παρακολούθηση (και άντληση δεδομένων καταγραφής - logs) συγκεκριμένων συστημάτων και εφαρμογών: • Συστήματα ασφαλείας: κατ΄ελάχιστο Firewalls, IPS, WAF, Content Security systems, VPNs, Vulnerability scanners, Antivirus , EDR, servers, NAC) • Συσκευές δικτύου: Τουλάχιστον Core switches, IP/MPLS nodes, Edge Routers, S/S FW, UDI devices	ΝΑΙ		

	• Λειτουργικά Συστήματα • Βάσεις Δεδομένων • Directory Services • Web Servers Applications (εμπορικές και μη – π.χ. custom εταιρικές εφαρμογές • Cloud Gateways: ERP, O365, EndPoint protection services, Cisco Umbrella, DUO MFA]			
2.8	Η προσφερόμενη υπηρεσία θα πρέπει να περιλαμβάνει ολοκληρωμένη υποδομή αποθήκευσης και ανάκτησης δεδομένων που να εξασφαλίζει την ακεραιότητα, την ανακτησιμότητα και τη διαθεσιμότητα των δεδομένων ασφαλείας.	ΝΑΙ		
2.9	Η προσφερόμενη υπηρεσία θα πρέπει να φιλτράρει τα δεδομένα καταγραφής πριν την τελική προώθησή τους στο κεντρικό σύστημα επεξεργασίας με σκοπό την απομάκρυνση των μη σχετικών με την ασφάλεια πληροφοριών και μείωση του όγκου δεδομένων που μεταφέρονται στο δίκτυο.	ΝΑΙ		
2.10	Να υποστηρίζονται κατ' ελάχιστον οι υπηρεσίες νέφους Microsoft Azure και Amazon. Να αναφερθούν άλλοι υποστηριζόμενοι κατασκευαστές.	ΝΑΙ		
2.11	Να παρέχεται κεντρική κονσόλα διαχείρισης (GUI) και παρακολούθησης των καταγεγραμμένων γεγονότων σε πραγματικό χρόνο.	ΝΑΙ		
2.12	Να προσφέρεται ομοιόμορφη διαμόρφωση (κανονικοποίηση) των δεδομένων καταγραφής ανεξαρτήτως του συστήματος προέλευσης και αποθήκευσης αυτών με την ίδια δομή με σκοπό την επιτάχυνση των μηχανισμών επεξεργασία, αναζήτησης και παραγωγής αναφορών (normalization).	ΝΑΙ		
2.13	Να προσφερθεί ομαδοποίηση των	ΝΑΙ		

	πηγών των logs ανά είδος πηγής (π.χ. web server, router).			
2.14	Να προσφερθεί υποστήριξη υπηρεσίας ευφυούς ανάλυσης απειλών (Threat Intelligence).	ΝΑΙ		
2.15	Η προτεινόμενη λύση να παρέχει υπηρεσία User Behavior Analysis. Να υποστηρίζονται κατ' ελάχιστον τα απαιτούμενα χαρακτηριστικά: • Δείκτης επικινδυνότητας ανά χρήστη • Λίστα παρακολούθησης χρηστών • Dashboard • Δυναμική και στατική παραμετροποίηση του δείκτη επικινδυνότητας Use Cases βασισμένα στην συμπεριφορά του χρήστη.	ΝΑΙ		
2.16	Η προτεινόμενη λύση να διαθέτει ενσωματωμένο σύστημα Machine Learning.	ΝΑΙ		
2.17	Να παρέχεται εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής και η παραγωγή σχετικών αναφορών με εφαρμογή ειδικών φίλτρων.	ΝΑΙ		
2.18	Να παρέχεται λεπτομερής εξέταση των γεγονότων καταγραφής που προκαλούν την ενεργοποίηση ενός κανόνα, με επιλογή γραφικής αναπαράστασης της σειράς των γεγονότων.	ΝΑΙ		
2.19	Να παρέχεται παράλληλη συλλογή και αποθήκευση δεδομένων καταγραφής τόσο σε πρωτογενή μορφή (raw data) όσο και σε κανονικοποιημένη μορφή (normalized).	ΝΑΙ		
2.20	Να παρέχεται εμφάνιση δεδομένων καταγραφής σε πραγματικό χρόνο.	ΝΑΙ		
2.21	Να παρέχεται εμφάνιση ιστορικών δεδομένων καταγραφής.	ΝΑΙ		
2.22	Να παρέχεται εμφάνιση μορφοποιημένων δεδομένων καταγραφής.	ΝΑΙ		

2.23	Να παρέχεται εμφάνιση αμορφοποίητων δεδομένων καταγραφής (raw).	ΝΑΙ		
2.24	Να παρέχεται αμεση διερεύνηση περιστατικών ασφάλειας σε πραγματικό χρόνο, μέσα από την παροχή των κατάλληλων εργαλείων διερεύνησης	ΝΑΙ		
2.25	Να παρέχεται δυνατότητα για απόκρυψη προσωπικής ευαίσθητης πληροφορίας από το περιβάλλον του χρήστη (Data Obfuscation), χωρίς να περιορίζεται καθόλου η δυνατότητα χρήσης του προϊόντος, για να εξασφαλίζεται η συμμόρφωση με τους κανονισμούς προστασίας δεδομένων προσωπικού χαρακτήρα. Να τεκμηριωθεί αναλυτικά.	ΝΑΙ		
2.26	Να παρέχεται εφαρμογή κανόνων συσχέτισης (correlation rules) σε πραγματικό χρόνο .	ΝΑΙ		
2.27	Παροχή έτοιμων κανόνων συσχέτισης για την άμεση ανάδειξη σημαντικών θεμάτων ασφάλειας της υποδομής.	ΝΑΙ		
2.28	Γρήγορη και εύκολη δημιουργία κανόνων συσχέτισης χρησιμοποιώντας ως βάση τους έτοιμους κανόνες που παρέχει η υπηρεσία.	ΝΑΙ		
2.29	Εφαρμογή κανόνων συσχέτισης δεδομένων καταγραφής από διαφορετικές πηγές (συστήματα και εφαρμογές).	ΝΑΙ		
2.30	Δημιουργία και αποστολή ειδοποιήσεων (alerts) σε καθορισμένους χρήστες,.	ΝΑΙ		
2.31	Η υπηρεσία θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων καταγραφής κατά την αποθήκευσή τους και να απαγορεύει την δυνατότητα διαγραφής/ τροποποίησης τους.	ΝΑΙ		
2.32	Να υποστηρίζονται κατ' ελάχιστο τα συγκεκριμένα πρωτόκολλα:	ΝΑΙ		

	• Syslog • OPSEC/ LEA Windows Security Event Protocol			
2.33	Να παρέχεται υποστήριξη γραφικού περιβάλλοντος (GUI) για την δημιουργία και διαχείριση αναφορών με βάση τα αποθηκευμένα αρχεία καταγραφής.	ΝΑΙ		
2.34	Να παρέχεται υποστήριξη ποικιλίας τύπων γραφημάτων για την δημιουργία αναφορών (πίνακες, μπάρες, πίτες, κλπ.)	ΝΑΙ		
2.35	Να παρέχεται υποστήριξη τυποποιημένων αναφορών για τις πιο συνήθεις κατηγορίες.	ΝΑΙ		
2.36	Να παρέχεται υποστήριξη τυποποιημένων προτύπων (templates) για εύκολη δημιουργία αναφορών κατ' επιλογή.	ΝΑΙ		
2.37	Να παρέχεται αυτοματοποιημένη παραγωγή αναφορών με χρονοπρογραμματισμό.	ΝΑΙ		
2.38	Να παρέχεται αυτοματοποιημένη αποστολή αναφορών σε χρήστες/ομάδες χρηστών μέσω e-mail.	ΝΑΙ		
2.39	Να είναι δυνατός ο καθορισμός διαφορετικών ρόλων διαχείρισης στη λύση με διαφορετικά δικαιώματα πρόσβασης.	ΝΑΙ		
2.40	Να παρέχεται διαχείριση σε επίπεδο γραμμής εντολής.	ΝΑΙ		
2.41	Να παρέχεται διαχείριση με γραφικό περιβάλλον (GUI).	ΝΑΙ		
2.42	Πρόσβαση διαχειριστών μέσω HTTPS και SSH.	ΝΑΙ		
2.43	Υποστήριξη δημιουργίας ευέλικτων προφίλ διαχειριστών με διαφορετικά δικαιώματα διαχείρισης.	ΝΑΙ		
2.44	Υποστήριξη αυτοματοποιημένης διερεύνησης περιστατικών ασφαλείας με την χρήση τεχνητής νοημοσύνης.	ΝΑΙ		
2.45	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει αυτόματα IOC mining στα	ΝΑΙ		

	περιστατικά ασφαλείας.			
2.46	Τα περιστατικά ασφαλείας θα πρέπει να συσχετιστούν με τις τακτικές και τις τεχνικές του πλαισίου MITRE ATT&CK.	ΝΑΙ		
2.47	Η προσφερόμενη υπηρεσία θα πρέπει να συγκρίνει τα περιστατικά ασφαλείας με προηγούμενα που έχουν αναλυθεί και να παρέχει στον αναλυτή πλήρη αναφορά.	ΝΑΙ		
2.48	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει προτεραιότητες στα περιστατικά με βάση τους Indicators Of Compromise (IOC), τους πόρους και τους κανόνες. Αυτή η ανάλυση μπορεί να εκπαιδευτεί από τον χρήστη επικυρώνοντας εάν συμφωνεί ή όχι με αυτή.	ΝΑΙ		
2.49	Η προσφερόμενη υπηρεσία θα πρέπει να δημιουργεί ένα γράφημα συσχετίσεων όλων των IOC που σχετίζονται με ένα περιστατικό.	ΝΑΙ		
2.50	Η προσφερόμενη υπηρεσία θα πρέπει να επιτρέπει την εξαγωγή των IOC σε σύνολα αναφοράς, CSV αρχεία ή Structured Threat Information eXpression (STIX) υπηρεσίες.	ΝΑΙ		
2.51	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει επιπλέον πληροφορίες ανά IOC έτσι ώστε να βοηθηθεί ο αναλυτής να αξιολογήσει το ρίσκο του.	ΝΑΙ		
2.52	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει συμβουλές αποκατάστασης και απόκρισης.	ΝΑΙ		
2.53	Περιγράψτε το περιεχόμενο που παρέχεται για συμβουλές αποκατάστασης - πηγές περιεχομένου, ανταγωνιστική διαφοροποίηση κ.λπ.	ΝΑΙ		
2.54	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει διεπαφές και δυνατότητες για αυτοματοποιημένη δράση.	ΝΑΙ		

Πίνακας-3. Αναλυτικές λειτουργικές προδιαγραφές Υπηρεσιών Διερεύνησης και Απόκρισης σε κυβερνοεπιθέσεις

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία Διερεύνησης και Απόκρισης σε κυβερνοεπιθέσεις				
3.1	Να προσφερθεί υπηρεσία τεχνητής νοημοσύνης για την διερεύνηση και την απόκριση σε κυβερνοεπιθέσεις ιδίου κατασκευαστή με την προσφερόμενη λύση SIEM. Να αναφερθεί ο κατασκευαστής και να πραγματοποιηθεί σχετική ανάλυση λειτουργίας	ΝΑΙ		
3.2	Υποστήριξη αυτοματοποιημένης διερεύνησης περιστατικών ασφαλείας με την χρήση τεχνητής νοημοσύνης.	ΝΑΙ		
3.3	Η προσφερόμενη λύση θα πρέπει να παρέχει αυτόματα IOC mining στα περιστατικά ασφαλείας.	ΝΑΙ		
3.4	Τα περιστατικά ασφαλείας θα πρέπει να συσχετιστούν με τις τακτικές και τις τεχνικές του πλαισίου MITRE ATT&CK	ΝΑΙ		
3.5	Η προσφερόμενη υπηρεσία θα πρέπει να συγκρίνει τα περιστατικά ασφαλείας με προηγούμενα που έχουν αναλυθεί και να παρέχει στον αναλυτή πλήρη αναφορά.	ΝΑΙ		
3.6	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει προτεραιότητες στα περιστατικά με βάση τους Indicators Of Compromise (IOC), τους πόρους και τους κανόνες. Αυτή η ανάλυση μπορεί να εκπαιδευτεί από τον χρήστη επικυρώνοντας εάν συμφωνεί ή όχι με αυτή.	ΝΑΙ		
3.7	Η προσφερόμενη υπηρεσία θα πρέπει να δημιουργεί ένα γράφημα συσχετίσεων όλων των IOC που σχετίζονται με ένα περιστατικό .	ΝΑΙ		
3.8	Η προσφερόμενη υπηρεσία θα πρέπει να επιτρέπει την εξαγωγή των IOC σε σύνολα αναφοράς, CSV αρχεία ή Structured Threat Information eXpression (STIX) υπηρεσίες.	ΝΑΙ		

3.9	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει επιπλέον πληροφορίες ανά IOC έτσι ώστε να βοηθηθεί ο αναλυτής να αξιολογήσει το ρίσκο του.	ΝΑΙ		
3.10	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει συμβουλές αποκατάστασης και απόκρισης.	ΝΑΙ		
3.11	Περιγράψτε το περιεχόμενο που παρέχεται για συμβουλές αποκατάστασης - πηγές περιεχομένου, ανταγωνιστική διαφοροποίηση κ.λπ.	ΝΑΙ		
3.12	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει διεπαφές και δυνατότητες για αυτοματοποιημένη δράση.	ΝΑΙ		
3.13	Ο υποψήφιος ανάδοχος θα πρέπει να παρέχει υπηρεσία απόκρισης 24x7 σε κυβερνοεπιθέσεις τοπικά ή απομακρυσμένα. Να αναφερθεί η μεθοδολογία λειτουργίας	ΝΑΙ		

Πίνακας-4. Αναλυτικές λειτουργικές προδιαγραφές Υπηρεσιών Ενορχήστρωσης και Αυτοματοποίησης των ροών εργασίας και των οδηγιών απόκρισης (playbooks)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία Ενορχήστρωσης και Αυτοματοποίησης των ροών εργασίας και των οδηγιών απόκρισης (playbooks)				
4.1	Να προσφερθεί υπηρεσία ενορχήστρωσης, αυτοματισμού και απόκρισης της ασφάλειας (SOAR).	ΝΑΙ		
4.2	Η προσφερόμενη υπηρεσία πρέπει να προσφέρει GUI για την διαχείριση.	ΝΑΙ		
4.3	Η προσφερόμενη υπηρεσία θα πρέπει να υποστηρίζει ταυτοποίηση των χρηστών μέσω LDAP.	ΝΑΙ		
4.4	Η προσφερόμενη υπηρεσία πρέπει να υποστηρίζει τη δημιουργία χρηστών και ομάδων χρηστών.	ΝΑΙ		
4.5	Η προσφερόμενη υπηρεσία θα πρέπει να παρέχει τη δυνατότητα παράδοσης πολλαπλών dashboard που μπορούν να προσαρμοστούν ώστε να πληρούν	ΝΑΙ		

	τις συγκεκριμένες απαιτήσεις διαφορετικών χρηστών του συστήματος.			
4.6	Η προσφερόμενη υπηρεσία πρέπει να διατηρεί μια βάση δεδομένων με τα περιστατικά ασφαλείας. Ο χρήστης θα πρέπει να είναι σε θέση να τα αναζητήσει.	ΝΑΙ		
4.7	Υποστήριξη ιστορικού ανά περιστατικό ασφαλείας.	ΝΑΙ		
4.8	Η προσφερόμενη υπηρεσία θα πρέπει να ενοποιείται με άλλες ευφυείς λύσεις ασφαλείας και δικτύου (security and network intelligence). Περιγράψτε το επίπεδο ολοκλήρωσης και τις υποστηριζόμενες λύσεις.	ΝΑΙ		
4.9	Υποστήριξη playbooks.	ΝΑΙ		
4.10	Η προσφερόμενη υπηρεσία πρέπει να επιτρέπει στους οργανισμούς να δοκιμάζουν διαδικασίες απόκρισης σε περιστατικά ασφαλείας, επιτρέποντάς τους να εντοπίζουν τα όποια σχεδιαστικά κενά και να βελτιώνουν τις διαδικασίες τους πριν συμβεί ένα πραγματικό συμβάν.	ΝΑΙ		
4.11	Υποστήριξη αυτόματης δημιουργίας τεκμηρίων διερεύνησης. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.12	Υποστήριξη αυτόματων σχέσεων μεταξύ περιστατικών με κοινά τεκμήρια. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.13	Υποστήριξη μακροπρόθεσμης ανάλυσης των τάσεων των περιστατικών ασφαλείας. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.14	Υποστήριξη περιοδικών ενημερώσεων των τεκμήριων ανά περιστατικών. Να περιγραφή αναλυτικά.	ΝΑΙ		
4.15	Υποστήριξη συσχετισμού των τεκμηρίων για διαφορετικά περιστατικά ασφαλείας. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.16	Δυνατότητα απόκρισης ανά	ΝΑΙ		

	περιστατικό. Για παράδειγμα, η λύση πρέπει να υποστηρίζει την ικανότητα αποκλεισμού ενός εισβολέα.			
4.17	Η λύση πρέπει να υποστηρίζει τη δυνατότητα συσχέτισης με ευφυείς πληροφορίες ασφαλείας (π.χ. geolocation, γνωστά κανάλια botnet, γνωστά εχθρικά δίκτυα κ.λπ.)	ΝΑΙ		
4.18	Υποστήριξη δυναμικής αύξησης των playbooks σε πραγματικό χρόνο για την υποστήριξη συγκεκριμένης ροής εργασιών. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.19	Η λύση θα πρέπει να παρέχει δυνατότητα στους αναλυτές να επανεξετάσουν τις πληροφορίες ενός περιστατικού ασφαλείας.	ΝΑΙ		
4.20	Η προσφερόμενη λύση πρέπει να παρέχει έτοιμα πρότυπα αναφορές για την δημιουργία αναφορών.	ΝΑΙ		
4.21	Υποστήριξη ροών εργασίας για τον αυτοματοποίηση της απόκρισης σε περιστατικά ασφαλείας. Να περιγραφεί αναλυτικά.	ΝΑΙ		
4.22	Υποστήριξη γραφημάτων των συμβάντων και των τεκμηρίων που σχετίζονται με κάθε περιστατικό, τα οποία μπορεί να βοηθήσουν στον εντοπισμό μιας ευρύτερης καμπάνιας ή μιας εξιδεικευμένης μόνιμης απειλής (APT).	ΝΑΙ		
4.23	Παρακολούθηση μετρικών και KPIs για συμβάντα και χρήστες, συμπεριλαμβανομένου του μέσου χρόνου ανίχνευσης (MTTD) και του μέσου χρόνου απόκρισης (MTTR).	ΝΑΙ		
4.24	Να παρέχεται επεξεργαστής γραφικής απεικόνισης των ροών εργασίας.	ΝΑΙ		
4.25	Να παρέχεται γραφική απεικόνιση των περιστατικών ασφαλείας.	ΝΑΙ		

Πίνακας-5. Αναλυτικές λειτουργικές προδιαγραφές Υπηρεσιών Ανίχνευσης και Απόκρισης (Endpoint Detection and Response -EDR)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία Endpoint Detection and Response (EDR)				
5.1	Να προσφερθεί εξειδικευμένο λογισμικό Endpoint Detection and Response (EDR) ως υπηρεσία (Managed Detection and Response).	ΝΑΙ		
5.2	Μέγιστος Αριθμός Τελικών Σημείων	>=2200		
5.3	Το προσφερόμενο λογισμικό θα πρέπει να υποστηρίζει τα παρακάτω λειτουργικά συστήματα της Microsoft: Windows 10 και 11 (32-bit, 64-bit versions), Windows Server 2016, 2019 ,2022 και 2025.	ΝΑΙ		
5.4	Το προσφερόμενο λογισμικό θα πρέπει να υποστηρίζει τα παρακάτω λειτουργικά συστήματα της Apple: MacOS Catalina (10.15), Big Sur (11.x) και Monterey (12.x).	ΝΑΙ		
5.5	Το προσφερόμενο λογισμικό θα πρέπει να υποστηρίζει κατ' ελάχιστον τα παρακάτω λειτουργικά συστήματα βασισμένα σε *nix: RedHat Enterprise Linux and CentOS 8.x, Ubuntu LTS 20.04.x, 22.04x server, 64-bit only Oracle Linux 7.7+, 8.2, SuSE SLES 15.1.	ΝΑΙ		
5.6	Το προσφερόμενο λογισμικό θα πρέπει να έχει 1% ή λιγότερο χρήση (utilization) CPU.	ΝΑΙ		
5.7	Το προσφερόμενο λογισμικό θα πρέπει να αναβαθμίζεται αυτόματα, χωρίς την παρεμβολή του τελικού χρήση καθώς και χωρίς να χρειάζεται επανεκκίνηση του συστήματος (τερματικός σταθμός ή διακομιστής).	ΝΑΙ		
5.8	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει προστασία "Anti-	ΝΑΙ		

	Tampering" και "Anti-violation" για την εφαρμογή λογισμικού (agent).			
5.9	Το προσφερόμενο λογισμικό δεν θα πρέπει να βασίζεται σε υπογραφές (signatures) για να την προστασία σε πραγματικό χρόνο από γνωστός απειλές, απεναντίας θα πρέπει να φέρει ενσωματωμένους μηχανισμούς Machine learning NGAV.	ΝΑΙ		
5.10	Το προσφερόμενο λογισμικό θα πρέπει να καταγράφει πληροφορίες σχετικές με τις διεργασίες, τους χρήστες, καθώς και όποια άλλη πληροφορία είναι σχετική με συμβάντα σε πραγματικό χρόνο.	ΝΑΙ		
5.11	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει προστασία έναντι ανεπιθύμητων ενεργειών που μπορεί να προκύψουν από τον τελικό χρήστη (όπως απεγκατάσταση).	ΝΑΙ		
5.12	Τόσο η εφαρμογή λογισμικού όσο και τα υπόλοιπα στοιχεία της λύσης θα πρέπει να είναι σε θέση να λειτουργούν και επικοινωνούν πίσω από proxy server.	ΝΑΙ		
5.13	Η εν λόγω υπηρεσία να ολοκληρώνεται με την υπηρεσία SOCaaS. Να περιγραφεί.	ΝΑΙ		
5.14	Να περιγραφεί αναλυτικά η υπηρεσία Managed Detection and Response (MDR).	ΝΑΙ		
5.15	Το προσφερόμενο λογισμικό θα πρέπει να λειτουργεί και σε "Offline" mode, ούτως ώστε να εξασφαλίζεται η ίδια λειτουργικότητα ακόμα και στις περιπτώσεις όπου η επικοινωνία με την υπόλοιπη υποδομή δεν είναι εφικτή.	ΝΑΙ		
5.16	Το προσφερόμενο λογισμικό θα πρέπει να εντοπίζει κάθε γνωστή κακόβουλη δραστηριότητα.	ΝΑΙ		
5.17	Το προσφερόμενο λογισμικό θα πρέπει να εντοπίζει διεργασίες που	ΝΑΙ		

	εκτελούνται, νέες διεργασίες, καθώς και αλληλεπίδραση ή παρεμπόδιση μεταξύ διεργασιών.			
5.18	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει δυνατότητα λήψης ενημερώσεων ανίχνευσης απειλών (threat detection updates).	ΝΑΙ		
5.19	Το προσφερόμενο λογισμικό θα πρέπει να υποστηρίζει δυνατότητα ταξινόμησης εντοπισθέντων συμβάντων, σύμφωνα με το επίπεδο σοβαρότητας του συμβάντος (Malicious, Suspicious, Inconclusive, Likely Safe, Potentially Unwanted Program or Application, Safe).	ΝΑΙ		
5.20	Το προσφερόμενο λογισμικό θα πρέπει να είναι σε θέση να συνυπάρξει με άλλες λύσεις ασφάλειας οι οποίες βρίσκονται στο τερματικό σύστημα (όπως άλλες λύσεις προστασίας από κακόβουλο λογισμικό).	ΝΑΙ		
5.21	Το προσφερόμενο λογισμικό θα πρέπει να δίνει τη δυνατότητα αποτροπής εκτέλεσης κακόβουλου εκτελέσιμου λογισμικού (malicious executables).	ΝΑΙ		
5.22	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να ελέγχει συσκευές USB και πόρτες.	ΝΑΙ		
5.23	Το προσφερόμενο λογισμικό θα πρέπει να εμποδίζει κακόβουλη κυκλοφορία η οποία σχετίζεται με τη διαρροή δεδομένων (data exfiltration).	ΝΑΙ		
5.24	Το προσφερόμενο λογισμικό θα πρέπει να εμποδίζει κακόβουλες συνδέσεις σε Command & Control (C&C) networks/servers.	ΝΑΙ		
5.25	Δυνατότητα Πρόληψης Έναντι Κακόβουλου Λογισμικού.			
5.26	Το προσφερόμενο λογισμικό θα πρέπει να αποκλείει, σε πραγματικό χρόνο, κάθε προσπάθεια κρυπτογράφηση αρχείων, ή τροποποίησης δεδομένων στο τερματικό σύστημα.	ΝΑΙ		

5.27	Το προσφερόμενο λογισμικό θα πρέπει να αποτρέπει οποιαδήποτε προσπάθεια κρυπτογράφησης του δίσκου από ransomware.	ΝΑΙ		
5.28	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να λειτουργεί και σε κατάσταση εκμάθησης (learning mode), κατά την οποία δεν εφαρμόζει πολιτικές αποτροπής σε πραγματικό χρόνο, αλλά καταγράφει τις κακόβουλες δραστηριότητες.	ΝΑΙ		
5.29	Το προσφερόμενο λογισμικό θα πρέπει να πραγματοποιεί περιοδικούς ελέγχους σε αρχεία (file scans) τόσο προγραμματισμένες όσο και κατ' απαίτηση (schedule ή on-demand), για τον εντοπισμό κακόβουλων αρχείων και τη δημιουργία ενός αποθετηρίου τύπου Threat Hunting.	ΝΑΙ		
5.30	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει μηχανισμό αυτοματοποιημένης απομόνωσης συσκευής/συσκευών κατά τον εντοπισμό δραστηριότητα κακόβουλου λογισμικού και σύμφωνα με το επίπεδο σοβαρότητας του ταξινομημένου κινδύνου.	ΝΑΙ		
5.31	Το προσφερόμενο λογισμικό θα πρέπει να αποκλείει με αυτοματοποιημένο τρόπο, ενέργειες που προκαλούνται κατά την εκτέλεση κακόβουλων αρχείων.	ΝΑΙ		
5.32	Το προσφερόμενο λογισμικό θα πρέπει να υποστηρίζει δυνατότητα δημιουργίας εξαιρέσεων (Whitelist/Blacklist) για την επικοινωνία εφαρμογών, οι οποίες θα πρέπει να βασίζονται σε hashes; MD5, SHA1, SHA256, όνομα αρχείου, διαδρομή (path) και πάροχο.	ΝΑΙ		
5.33	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να συνεργαστεί με το προσφερόμενο λογισμικό Security	ΝΑΙ		

	Information and Event Management (SIEM) ως υπηρεσία.			
5.34	Το προσφερόμενο λογισμικό θα πρέπει να είναι σε θέσει να ανακτήσει μέρος της μνήμης ή ολόκληρη της διεργασία από τη μνήμη, ούτως ώστε να πραγματοποιηθεί η δικανική ανάλυση.	ΝΑΙ		
5.35	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να σβήνει με αυτοματοποιημένο τρόπο, κακόβουλα αρχεία.	ΝΑΙ		
5.36	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να επαναφέρει τα δεδομένα εκείνα που τροποποιήθηκαν από κακόβουλη δραστηριότητα.	ΝΑΙ		
5.37	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να περιορίζει την πρόσβαση εφαρμογών στο δίκτυο, βάσει της ταξινόμησης της εφαρμογής, η οποία έχει πραγματοποιηθεί λαμβάνοντας υπόψη βαθμολογίες φήμης (reputation score).	ΝΑΙ		
5.38	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει δυνατότητα λήψης και αναπαράστασης όλης της "αλυσίδας" επίθεσης και των κακόβουλων δραστηριοτήτων.	ΝΑΙ		
5.39	Το προσφερόμενο λογισμικό θα πρέπει μέσω συνεργασίας με sandbox λύση, να υποβάλλει τα εκτελέσιμα αρχεία στη λύση sandbox για περαιτέρω ανάλυση και αξιολόγηση.	ΝΑΙ		
5.40	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει πολλαπλούς αυτοματοποιημένους μηχανισμούς προστασίας, όπως τερματισμός κακόβουλος διεργασιών, διαγραφή κακόβουλων αρχείων, αποτροπή σύνδεσης εφαρμογών στο δίκτυο.	ΝΑΙ		
5.41	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να ανακαλύψει εφαρμογές με ευπάθειες, οι οποίες προσπαθούν να επικοινωνήσουν με το δίκτυο.	ΝΑΙ		

5.42	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει τη δυνατότητα Virtual Patching, περιορίζοντας με αυτόν τον τρόπο την αμφίδρομη επικοινωνία των "ευάλωτων" ευπαθειών.	ΝΑΙ		
5.43	Το προσφερόμενο λογισμικό θα πρέπει να είναι σε θέση να μειώσει το Endpoint Attack Surface, χρησιμοποιώντας πολιτικές επικοινωνίας ελέγχου για εφαρμογές, βάσει συγκεκριμένων CVEs ή/και φήμης (reputation).	ΝΑΙ		
5.44	Το προσφερόμενο λογισμικό θα πρέπει να είναι σε θέση να αποτρέψει την επικοινωνία οποιασδήποτε εφαρμογής με μη εξουσιοδοτημένα δίκτυα.	ΝΑΙ		
5.45	Το προσφερόμενο λογισμικό θα πρέπει να είναι σε θέση να αποτρέψει την επικοινωνία μίας εφαρμογής, βάσει της έκδοσης της συγκεκριμένης εφαρμογής.	ΝΑΙ		
5.46	Το προσφερόμενο λογισμικό θα πρέπει να μπορεί να ανακαλύψει όλες τις εφαρμογές που προσπαθούν να επικοινωνήσουν εκτός τους τερματικού σταθμού.	ΝΑΙ		
5.47	Το προσφερόμενο λογισμικό θα πρέπει να εντοπίζει και να αποτρέπει προσπάθειες τύπου κλιμάκωσης δικαιωμάτων πρόσβασης (privileges elevation).	ΝΑΙ		
5.48	Το προσφερόμενο λογισμικό θα πρέπει να αποτρέπει επιθέσεις τύπου ransomware.	ΝΑΙ		
5.49	Το προσφερόμενο λογισμικό θα πρέπει να συμμορφώνεται με διεθνή πρότυπα ασφάλειας και πρότυπα κανονιστικής συμμόρφωσης όπως ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ).	ΝΑΙ		
5.50	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει κεντρική πλατφόρμα διαχείρισης, η οποία να	ΝΑΙ		

	είναι σε θέση να ενοποιηθεί (integration) με Active Directory, καθώς επίσης και να παρέχει δυνατότητα 2-Factor Authentication.			
5.51	Η κεντρική πλατφόρμα διαχείρισης θα πρέπει να παρέχει διαφορετικούς τύπους πρόσβασης, βάσει των δικαιωμάτων πρόσβασης του χρήστη.	ΝΑΙ		
5.52	Η κεντρική κονσόλα διαχείρισης θα πρέπει να παρέχει Full Restful API interface για ενοποίηση με εξωτερικά συστήματα.	ΝΑΙ		
5.53	Το προσφερόμενο λογισμικό θα πρέπει να παρέχει μία αρχιτεκτονική διαχείρισης μέσω του Cloud, χωρίς να απαιτείται καμία on-premise υπηρεσία. Ταυτόχρονα θα πρέπει να δίνει την επιλογή on-premise υλοποίησης.	ΝΑΙ		
5.54	Η κεντρική κονσόλα διαχείρισης θα πρέπει να επισημαίνει τα συμβάντα εκείνα που χρήζουν περαιτέρω ανάλυσης.	ΝΑΙ		
5.55	Η κεντρική κονσόλα διαχείρισης θα πρέπει να παρέχει πληροφορίες σχετικά με την κατάσταση των εγκατεστημένων εφαρμογών λογισμικού (agents).	ΝΑΙ		
5.56	Η κεντρική κονσόλα διαχείρισης θα πρέπει να επιτρέπει την ενοποίηση με SMTP για την αποστολή ειδοποίησης μέσω υπηρεσίας email.	ΝΑΙ		
5.57	Η κεντρική κονσόλα διαχείρισης θα πρέπει να παρέχει μηχανισμό καταγραφής των δραστηριοτήτων των χρηστών, για τις αλλαγές που πραγματοποιούν στο σύστημα. Τα αρχεία καταγραφής αυτά (audit trails) θα πρέπει να μπορούν να εξαχθούν σε CSV format.	ΝΑΙ		
5.58	Το προσφερόμενο λογισμικό θα πρέπει να ενημερώνεται αυτόματα, από τον επίσημο ιστοχώρο του	ΝΑΙ		

	κατασκευαστή με πρόσφατες υπογραφές (signatures) ούτως ώστε να είναι σε θέση να εντοπίζει και να αποτρέπει σύγχρονες επιθέσεις.			
5.59	Ο ανάδοχος θα αναλάβει την απεγκατάσταση της υφιστάμενης λύσης EDR, την εγκατάσταση της προσφερόμενης και την μεταφορά των πολιτικών και κανόνων που υπάρχουν (policies, exceptions, whitelisting, groups) από την υφιστάμενη στη νέα υποδομή.	ΝΑΙ		

Πίνακας-6. Αναλυτικές λειτουργικές προδιαγραφές Υπηρεσίας ευφυών πληροφοριών απειλών (Cyber Threat Intelligence)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ
Υπηρεσία Cyber Threat Intelligence				
6.1	Ο MSS Provider θα πρέπει να μπορεί να παρέχει και υπηρεσίες dark web monitoring, με ενεργή σάρωση σε forums, marketplaces και άλλες πηγές του underground web για απειλές ή αναφορές που στοχεύουν τον οργανισμό, τους υπαλλήλους ή τους πελάτες του.	ΝΑΙ		
6.2	Ο MSS Provider υποχρεούται να παρέχει curated threat intelligence σχετικά με threat actors, malware families και indicators of compromise (IOCs) που είναι συναφή με τον οργανισμό. Το threat intelligence πρέπει να ενημερώνεται τακτικά και να παραδίδεται μέσω μηνιαίων Threat Landscape Reports, τα οποία θα περιλαμβάνουν πληροφορίες για τις τρέχουσες και αναδυόμενες απειλές που επηρεάζουν τον κλάδο του οργανισμού.	ΝΑΙ		
6.3	Η πλατφόρμα που θα χρησιμοποιεί ο	ΝΑΙ		

	MSSP θα πρέπει να είναι συμμορφούμενη με το ISO27001			
6.4	Η λύση θα πρέπει να έχει δυνατότητες ανίχνευσης credentials που έχουν διαρρεύσει με βάση τις δυνατότητες text mining.	ΝΑΙ		
6.5	Η λύση θα πρέπει να έχει δυνατότητες ανίχνευσης των προσωπικών δεδομένων των εργαζομένων που διαρρέουν στο διαδίκτυο.	ΝΑΙ		
6.6	Η λύση θα πρέπει να έχει δυνατότητες ανίχνευσης αναφορών σε μυστικά έργα που σχετίζονται με περιουσιακά στοιχεία της υπηρεσίας.	ΝΑΙ		
6.7	Η λύση θα πρέπει να έχει δυνατότητες αναφοράς για την πρόθεση στόχευσης οργανισμών.	ΝΑΙ		
6.8	Η λύση θα πρέπει να έχει δυνατότητες αναφοράς για μεγάλες hacktivism καμπάνιες.	ΝΑΙ		
6.9	Η λύση θα πρέπει να περιλαμβάνει την παρακολούθηση φόρουμ και κλειστών κοινοτήτων.	ΝΑΙ		
6.10	Η λύση πρέπει να καλύπτει εξειδικευμένα αγορές όπως αγορές botnet και παρόμοιες πλατφόρμες.	ΝΑΙ		
6.11	Η λύση πρέπει εν δυνάμει να μπορεί να υποστηρίξει Takedowns.	ΝΑΙ		
6.12	Η λύση θα πρέπει να εκδίδει ειδοποιήσεις σχετικά με διαπιστευτήρια VIP που διαρρέουν στο διαδίκτυο.	ΝΑΙ		
6.13	Η λύση θα πρέπει να εντοπίζει περιπτώσεις διαρροής ευαίσθητων δεδομένων σε deep και dark web.	ΝΑΙ		
6.14	Η λύση θα πρέπει να εντοπίζει παραβιασμένους λογαριασμούς υπαλλήλων του οργανισμού.	ΝΑΙ		
6.15	Η λύση να επιτρέπει την αποστολή email alerts για custom queries.	ΝΑΙ		
6.16	Η λύση να υποστηρίζει την εξαγωγή CSV για εύκολο χειρισμό δεδομένων.	ΝΑΙ		
6.17	Η λύση θα πρέπει να έχει δυνατότητα	ΝΑΙ		

	συνεχούς παρακολούθησης για ζητούμενες λέξεις-κλειδιά.			
6.18	Η λύση θα πρέπει να έχει αυτοματοποιημένη ταξινόμηση σοβαρότητας επί των ειδοποιήσεων/συμβάντων.	ΝΑΙ		
6.19	Η λύση θα πρέπει να επιτρέπει την παρακολούθηση των διευθύνσεων IP που ανήκουν στον οργανισμό.	ΝΑΙ		
6.20	Η λύση θα πρέπει να επιτρέπει την παρακολούθηση των διευθύνσεων ηλεκτρονικού ταχυδρομείου που ανήκουν στον οργανισμό.	ΝΑΙ		
6.21	Η λύση πρέπει να διασφαλίζει δυνατότητες συλλογής δεδομένων σε περισσότερες από 1 γλώσσες.	ΝΑΙ		

4 SLA MSS/SOC

Στην περίπτωση που κατά την διάρκεια της παροχής των υπηρεσιών από τον ανάδοχο συμβεί κάποιο περιστατικό ασφαλείας, θα πρέπει να τηρηθούν τα όσα περιγράφονται στην παράγραφο 2 Τεχνική Περιγραφή ζητούμενης υπηρεσίας SOC και στους πίνακες συμμόρφωσης του παρόντος παραρτήματος.

Ως περιστατικό ασφαλείας υψίστης σημασίας, ορίζεται αυτό το οποίο προκαλεί, ή μπορεί να προκαλέσει κατά περίπτωση, απώλεια δεδομένων της ΕΡΤ Α.Ε., ή οικονομική ζημιά. Σε περίπτωση ασυμφωνίας των δύο πλευρών σχετικά με τον χρόνο απόκρισης ως αποδεικτικά θα μπορούν να ισχύσουν αρχεία κλήσεων, timestamps emails και SMS.

5 Λοιπά στοιχεία έργου.

Συνεργασία υποψηφίου με το προσωπικό της ΕΡΤ Α.Ε.

Ο υποψήφιος δηλώνει ότι θα συνεργαστεί στο μέγιστο βαθμό με το προσωπικό της ΕΡΤ Α.Ε. που θα υποδειχθεί από την τελευταία για την ολοκλήρωση του έργου, θέτοντας υπόψη του προσωπικού της ΕΡΤ Α.Ε. κάθε στοιχείο που έχει στην αντίληψή του και αφορά το έργο, συμπεριλαμβανομένου κάθε στοιχείου που μπορεί να συμβάλει στην καλυτέρευση, την επίσπευση, ή την βελτιστοποίηση του έργου, καθώς και κάθε τυχόν στοιχείου που αντίθετα, μπορεί να θέσει την ποιότητα ή τις προθεσμίες παράδοσης του έργου σε κίνδυνο.

Βλαβοληψία και διαχείριση βλαβών:

1. Ο υποψήφιος θα πρέπει να διαθέτει βλαβοληπτικό κέντρο με συνεχή λειτουργία 24×7×365 και να προσφέρει πρόσβαση σε αυτό μέσω αριθμού σταθερού τηλεφώνου, αριθμού κινητού τηλεφώνου και μέσω email.
2. Προσφέρεται προς την ΕΡΤ Α.Ε. πρόσβαση στα συστήματα διαχείρισης βλαβών του κατασκευαστή του εξοπλισμού και λογισμικού που προσφέρεται στο έργο.
3. Για τις βλάβες για τις οποίες απαιτείται επικοινωνία με τεχνικό, ο υποψήφιος προσφέρει σε βάση 24×7×365 χρόνο κλήσης της ΕΡΤ Α.Ε. από τεχνικό του (call-back) μικρότερο της μίας ώρας.
4. Για τις δυσλειτουργίες για τις οποίες απαιτείται επιτόπια επίσκεψη τεχνικού του, ο υποψήφιος θα πρέπει να προσφέρει χρόνο επιτόπιας επίσκεψης του τεχνικού μικρότερο των 2 ωρών.

6 Χρονοδιαγράμματα

Το ανώτατο χρονικό διάστημα για την παράδοση από τον ανάδοχο, όλων των ζητούμενων υπηρεσιών, ορίζεται σε εξήντα (60) ημέρες από την υπογραφή της σύμβασης. Εντός αυτού του διαστήματος, ο ανάδοχος οφείλει:

- Να εγκαταστήσει στο δίκτυο της ΕΡΤ Α.Ε. όλες τις αναγκαίες μηχανές (εικονικές ή φυσικές) για τη λειτουργία της υπηρεσίας SOC.
- Να εντάξει όλα τα απαραίτητα log sources στα συστήματα.
- Να ολοκληρώσει την απεγκατάσταση του υφιστάμενου EDR και να εγκαταστήσει το προσφερόμενο.
- Να παρέχει εκπαίδευση στο αρμόδιο προσωπικό της ΕΡΤ Α.Ε. σχετικά με το προσφερόμενο portal και τη διαχειριστική κονσόλα του EDR.
    - 2 Group 7 ατόμων για το portal από 10 ώρες έκαστο
    - 2 Group 7 ατόμων για το EDR από 10 ώρες έκαστο
- Να πραγματοποιήσει τις απαιτούμενες ρυθμίσεις στους αυτοματοποιημένους μηχανισμούς συσχετισμού απειλών.
- Να πραγματοποιήσει όλες τις απαραίτητες ρυθμίσεις και παραμετροποιήσεις για την πλήρη λειτουργία των προσφερόμενων υπηρεσιών.

Η έναρξη παροχής των υπηρεσιών θα λάβει χώρα την επόμενη ημέρα από την παραλαβή τους από την αρμόδια επιτροπή και η διάρκεια των υπηρεσιών θα είναι τρία (3) έτη από εκείνη τη χρονική στιγμή.
Ο ανάδοχος υποχρεούται να συνεργαστεί με το προσωπικό της ΕΡΤ Α.Ε. για την ολοκλήρωση του έργου. Σε περίπτωση τεκμηριωμένης καθυστέρησης που

αποδίδεται στο προσωπικό της ΕΡΤ Α.Ε., το αντίστοιχο χρονικό διάστημα δεν θα συνυπολογίζεται στο συνολικό χρόνο των εξήντα (60) ημερών. Ως καθυστέρηση υπαιτιότητας της ΕΡΤ Α.Ε. θεωρείται η μη έγκαιρη παροχή απαραίτητων στοιχείων για την υλοποίηση του έργου, όπως καταγραφές συστημάτων, δικαιώματα πρόσβασης, δημιουργία λογαριασμών υπηρεσίας και εικονικών μηχανών.

7 Διαγωνιστική διαδικασία - Αξιολόγηση προσφορών

Η Αξιολόγηση θα γίνει βάσει συμφερότερης από οικονομικής απόψεως προσφοράς με βάση την τιμή.

7.1 Τεχνική αξιολόγηση

Στο στάδιο της τεχνικής αξιολόγησης οι προσφορές των υποψηφίων εξετάζονται ως προς την αρτιότητα, την πληρότητα, τη συμφωνία με τις προδιαγραφές και την τήρηση των όρων που χαρακτηρίζονται απαράβατοι στην παρούσα. Προσφορές που δεν πληρούν έστω και έναν απαράβατο όρο, ή είναι με άλλο τρόπο μη συμβατές με τις προδιαγραφές ή αποκλίνουν ουσιωδώς από αυτές, απορρίπτονται σε αυτό το στάδιο και δεν αξιολογούνται περαιτέρω. Όλοι οι όροι των πινάκων συμμόρφωσης της ενότητας 2 του παραρτήματος τεχνικών προδιαγραφών είναι απαράβατοι.

7.2 Οικονομική αξιολόγηση

Στο στάδιο της οικονομικής αξιολόγησης εξετάζονται οι οικονομικές προσφορές όσων υποψηφίων συνεχίζουν να συμμετέχουν στο διαγωνισμό. Η αξιολόγηση γίνεται βάσει του παρακάτω πίνακα, στον οποίον πρέπει υποχρεωτικά και επί ποινή αποκλεισμού να έχουν συμπληρωθεί τα ζητούμενα στοιχεία. Όλες οι τιμές πρέπει να είναι σε Ευρώ με δύο δεκαδικά ψηφία. Όλες οι αναφερόμενες τιμές πρέπει να είναι χωρίς ΦΠΑ και ο ΦΠΑ πρέπει να προστίθεται στο τέλος, όπως στον πίνακα που ακολουθεί. Τυχόν κόστος αρχικής εγκατάστασης του υποψήφιου αναδόχου, θα ενσωματωθεί στο μηνιαίο κόστος των υπηρεσιών και δεν θα αναφέρεται διακριτά. Διακριτά θα αναφέρεται η τιμή του λογισμικού

Σύμβολο	**Αντικείμενο**	**Ποσό**
K_1	Μηνιαία τιμή υπηρεσίας SOC MSS 24x7 (χωρίς ΦΠΑ)	€ ,
K_{edr}	Μηνιαία τιμή λογισμικού EDR για 2000 endpoints (χωρίς ΦΠΑ)	€ ,
Kt	Κόστος εκπαίδευσης	€ ,
K_{CTI}	Μηνιαία τιμή λογισμικού Cyber Threat Intelligence	€ ,
K	Τιμή προσφοράς	€ ,
$Φ$	ΦΠΑ που αντιστοιχεί στο κόστος υπηρεσιών K_1, K_{edr}, K_{CTI} για	€ ,

	3 έτη	

Την τιμή προσφοράς *Κ* θα πρέπει ο υποψήφιος να την συμπληρώσει στον προηγούμενο πίνακα, υπολογίζοντάς την βάσει του τύπου:

$$\mathbf{K = 36 \times (K_1 + K_{edr} + K_{CTI}) + Kt}$$

Εάν η τιμή προσφοράς Κ υπερβαίνει το ποσό του προϋπολογισμού του έργου, η οικονομική προσφορά του υποψηφίου απορρίπτεται και δεν αξιολογείται περαιτέρω.

Ο ΦΠΑ *Φ* θα πρέπει να αντιστοιχεί στο κόστος της παροχής των υπηρεσιών (***K*$_1$**,***Kedr***, ***K*$_{CTI}$**) για τρία έτη και θα πρέπει να έχει υπολογιστεί με τους τυπικούς κανόνες στρογγυλοποίησης δεκαδικών (π.χ., 12,345 → 12,35 ενώ 21,234 → 21,23).

7.3 Αξιολόγηση συμφερότερης προσφοράς

Η κατακύρωση της προμήθειας θα γίνει με κριτήριο ανάθεσης την πλέον συμφέρουσα από οικονομικής απόψεως προσφορά, με βάση μόνο την τιμή.
Ως συμφερότερη θα θεωρηθεί η προσφορά εκείνη που έχει το μικρότερο Κ.

8 Τεχνική και Επαγγελματική ικανότητα

Όσον αφορά στην τεχνική και επαγγελματική ικανότητα για την παρούσα διαδικασία σύναψης σύμβασης, λόγω του εξειδικευμένου χαρακτήρα των αντικειμένων της υπό ανάθεση σύμβασης, οι οικονομικοί φορείς απαιτείται:

Α. Να διαθέτουν τις κατάλληλες εγκαταστάσεις και τεχνικό εξοπλισμό για να παρέχουν τις υπηρεσίες της σύμβασης. Ειδικότερα απαιτείται να διαθέτουν και να λειτουργούν εξειδικευμένο Επιχειρησιακό Κέντρο Ασφάλειας (SOC) με τα κάτωθι τουλάχιστον χαρακτηριστικά:

- Λειτουργία 24x7 τουλάχιστον για μία πενταετία.
- Παροχή υπηρεσιών διαχείρισης περιστατικών ασφαλείας 24x7 σε πραγματικό χρόνο (Real Time Threat Management) με χρήση λογισμικού SIEM. Να αναφερθούν λεπτομερώς.
- Παροχή υπηρεσιών ανίχνευσης και απόκρισης (Managed Detection and Response) με χρήση λογισμικού EDR. Να αναφερθούν λεπτομερώς.
- Να παρέχουν υπηρεσία Cyber Threat Intelligence σε τουλάχιστον πέντε (5) οργανισμούς.

Β. Ο Ανάδοχος θα πρέπει να διαθέτει αποδεδειγμένη εμπειρία στην παροχή υπηρεσιών παρακολούθησης και διαχείρισης περιστατικών ασφάλειας πληροφοριών κατά την τελευταία πενταετία.
Η εμπειρία αυτή να τεκμηριώνεται με την επιτυχή εκτέλεση έργων σε δημόσιους ή ιδιωτικούς οργανισμούς, συνολικής κλίμακας και πολυπλοκότητας αντίστοιχης με τις απαιτήσεις του παρόντος διαγωνισμού.
Ο Ανάδοχος θα πρέπει να υποβάλει ενδεικτικό κατάλογο έργων που παρουσιάζουν επάρκεια σε όγκο, πολυπλοκότητα και λειτουργικό αντικείμενο συναφές με την παρούσα διακήρυξη.
Στο σύνολο των έργων που θα υποβληθούν θα πρέπει να περιλαμβάνονται τουλάχιστον οι παρακάτω συμβάσεις

- Μία (1) τουλάχιστον να έχει πραγματοποιηθεί σε συνθήκες ρυθμαπόδοσης τουλάχιστον 2.500 eps.
- Τρεις (3) τουλάχιστον που να συμπεριλαμβάνουν αυτοματοποιημένη διερεύνηση περιστατικών ασφαλείας και παροχή υπηρεσιών MDR σε εταιρείες / οργανισμούς με πάνω από 1000 endpoints.

Γ. Οι οικονομικοί φορείς για την παρούσα διαδικασία σύναψης σύμβασης οφείλουν να συμμορφώνονται με τα παρακάτω πρότυπα διασφάλισης ποιότητας :

- ISO 9001:2015 για τη Διαχείριση της Ποιότητας, ή ισοδύναμο, εν ισχύ, από διαπιστευμένο Οργανισμό

- ISO 27001:2022 για την Ασφάλεια των Πληροφοριών ή αντίστοιχο ή ισοδύναμο, εν ισχύ, από διαπιστευμένο Οργανισμό

- ISO 14001:2015 για Σύστημα Περιβαλλοντικής Διαχείριση ή ισοδύναμο, εν ισχύ, από διαπιστευμένο Οργανισμό

- ISO 20000-1:2018 Παροχή υπηρεσιών σχεδιασμού, εγκατάστασης, τεχνικής υποστήριξης, διαχειριζόμενων υπηρεσιών ασφαλείας (SOC), υπηρεσιών ασφάλειας πληροφοριών συστημάτων πληροφορικής

- ISO 22301:2019 Συστήματος Διαχείρισης Επιχειρησιακής Συνέχειας (Business Continuity Management System), ή ισοδύναμο, εν ισχύ, από διαπιστευμένο Οργανισμό.

Σε περίπτωση ένωσης, οι παραπάνω απαιτήσεις πρέπει να καλύπτονται απ’ όλα τα μέλη της ένωσης.

Η Αναθέτουσα Αρχή αναγνωρίζει ισοδύναμα πιστοποιητικά που έχουν εκδοθεί από φορείς διαπιστευμένους από ισοδύναμους Οργανισμούς διαπίστευσης, εδρεύοντες και σε άλλα κράτη – μέλη, σύμφωνα με τον Κανονισμό 765/2008. 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.

Δ. Οι οικονομικοί φορείς που συμμετέχουν στη διαδικασία σύναψης της παρούσας απαιτείται, επιπροσθέτως, να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου η οποία να αποτελείται τουλάχιστον από :

- Έναν (1) Υπεύθυνο έργου, ο οποίος να διαθέτει :
    - Βασικό τίτλο σπουδών, πτυχίο ή δίπλωμα Ανώτατου Εκπαιδευτικού Ιδρύματος (ΑΕΙ), ή Ελληνικού Ανοικτού Πανεπιστημίου (ΕΑΠ) ΑΕΙ, αναγνωρισμένο ισότιμο αντίστοιχης ειδικότητας σχολών της αλλοδαπής στο γνωστικό αντικείμενο που έχει άμεση συνάφεια με τον τύπο των παρεχόμενων υπηρεσιών, στο πλαίσιο του Έργου.
    - Τουλάχιστον 10ετή επαγγελματική εμπειρία σε Διοίκηση αντικειμένου ως Υπεύθυνος Έργου, και
    - Πιστοποίηση PMP ή αντίστοιχη.

- Έναν (1) Αναπληρωτή Υπεύθυνο έργου ο οποίος θα αποτελεί εφεδρικό PM σε περίπτωση μη διαθεσιμότητας του κύριου, ο οποίος να διαθέτει :
    - Πτυχίο πανεπιστημιακής εκπαίδευσης (Πτυχίο ΑΕΙ/ΑΤΕΙ) και μεταπτυχιακό τίτλο σπουδών.
    - Γενική επαγγελματική εμπειρία τουλάχιστον δέκα (10) ετών και εξειδικευμένη επαγγελματική εμπειρία τουλάχιστον οκτώ (8) ετών σε Διαχείριση και Διοίκηση Έργων,
    - Συμμετοχή, με ρόλο Υπεύθυνου ή Αναπληρωτή Υπεύθυνου έργου, σε τουλάχιστον 5 έργα στο αντικείμενο της ασφάλειας πληροφοριακών συστημάτων, και

- Έναν (1) σύμβουλο Ασφάλειας Πληροφοριών, οι οποίος να διαθέτει:
    - Πτυχίο πανεπιστημιακής εκπαίδευσης (Πτυχίο ΑΕΙ/ΑΤΕΙ) και μεταπτυχιακό τίτλο σπουδών στην ασφάλεια πληροφοριακών

συστημάτων.
- Εξειδικευμένη επαγγελματική εμπειρία τουλάχιστον οκτώ (8) ετών σε θέματα ασφάλειας πληροφοριών ή σχεδιασμό και υλοποίηση πολιτικών ασφάλειας.
- Συμμετοχή σε τουλάχιστον πέντε (5) αντίστοιχα έργα στο αντικείμενο της ασφάλειας πληροφοριών.
- Τουλάχιστον τις ακόλουθες πιστοποιήσεις : ISO/IEC 27001:2022 Lead Auditor, ISO 22301:2019 Lead Auditor

- Δύο (2) Διαχειριστές Συστημάτων Ασφάλειας (SIEM) οι οποίοι θα διαθέτουν :
  - Πτυχίο πανεπιστημιακής εκπαίδευσης (Πτυχίο ΑΕΙ/ΑΤΕΙ) Θετικής κατεύθυνσης
  - Εξειδικευμένη επαγγελματική εμπειρία τουλάχιστον έξη (6) ετών στη διαχείριση συστημάτων ασφάλειας,.
  - Συμμετοχή σε τουλάχιστον πέντε (5) έργα που σχετίζονται με την εγκατάσταση ή διαχείριση συστημάτων ασφάλειας πληροφοριών.

- Τέσσερις (4) Μηχανικούς Δικτύου , Προστασίας τερματικών , Ασφάλειας Δεδομένων, οι οποίοι θα διαθέτουν :
  - Πτυχίο πανεπιστημιακής εκπαίδευσης (Πτυχίο ΑΕΙ/ΑΤΕΙ) Θετικής κατεύθυνσης
  - Εξειδικευμένη επαγγελματική εμπειρία τουλάχιστον πέντε (5) ετών διαχείριση δικτύων και επικοινωνιών.

Εμπειρία σε τουλάχιστον Πέντε (5) έργα που περιλαμβάνουν την εγκατάσταση ή υποστήριξη δικτυακών υποδομών ή υπηρεσιών επικοινωνιών ή προστασίας τερματικών ή ασφάλειας πληροφοριών

- Το SOC να διαθέτει τουλάχιστον 15 αναλυτές επιπέδου 1, επιπέδου 2 και επιπέδου 3, από τους οποίους τουλάχιστον 10 αναλυτές να ανήκουν στο μόνιμο προσωπικό του αναδόχου κατά τα τελευταία 3 έτη. Να παραδοθούν σχετικά έγγραφα τεκμηρίωσης. Οι 10 αναλυτές να διαθέτουν κατάλληλα πιστοποιητικά network security analyst. Αναλυτικότερα τουλάχιστον 4 tier 1 security analysts να διαθέτουν **CompTIA Security+** ή **GIAC Information Security Fundamentals (GISF),** τουλάχιστον 4 tier 2 security analysts να διαθέτουν **CompTIA CySA+ ή GIAC Security Essentials (GSEC) ή C-Council Certified SOC Analyst (CSA)** και τουλάχιστον

2 tier 3 security analysts να διαθέτουν **CISSP ή CISA ή GIAC Certified Incident Handler**

Σε περίπτωση ένωσης, οι παραπάνω απαιτήσεις μπορούν να καλύπτονται αθροιστικά από τα μέλη της ένωσης. Επιπλέον έκαστο μέλος της προτεινόμενης ομάδας έργου του Υποψηφίου Αναδόχου δεν μπορεί να καλύψει πάνω από έναν από τους παραπάνω ζητούμενους ρόλους.

9 Τρόπος πληρωμής – Προϋπολογισμός Έργου

Η υπηρεσία θα εξοφλείται κατά τη διάρκεια της σύμβασης των τριών ετών τμηματικά. Η έναρξη των υπηρεσιών θα οριστεί την επομένη της ημερομηνίας παραλαβής του συνόλου των υπηρεσιών από την αρμόδια επιτροπή παραλαβής και θα έχει διάρκεια τρία (3) έτη. Η τιμολόγηση θα γίνεται ανά μήνα ή ανά τρίμηνο μετά την παροχή της υπηρεσίας και θα εξοφλείται εντός 30 ημερών από την ημερομηνία τιμολόγησης και βεβαίωσης από την αρμόδια επιτροπή παραλαβής και παρακολούθησης.
Ο προϋπολογισμός του έργου για διάρκεια τριών ετών ορίζεται στο ποσό των **450.000,00€ πλέον ΦΠΑ**.