ΠΑΡΑΡΤΗΜΑ Ι

ΕΡΓΟ: Προμήθεια, εγκατάσταση και λειτουργία ολοκληρωμένης υποδομής κυβερνοασφάλειας για τις ανάγκες του έργου DEP: Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC), συγχρηματοδοτούμενο από το Πρόγραμμα DEP (No 101127713), με κωδικό ΣΑΕ 0632 και κωδικό ενάριθμο έργου 2025ΣΕ063200005.

1. ΓΕΝΙΚΑ

1. Το παρόν παράρτημα συνοδεύει την πρόσκληση προκαταρκτικής διαβούλευσης για την προμήθεια, εγκατάσταση και λειτουργία ολοκληρωμένης υποδομής κυβερνοασφάλειας, για την ανάπτυξη και αναβάθμιση του Ελληνικού Επιχειρησιακού Κέντρου Ενοποιημένης Ασφάλειας.

1. Σκοπός του έργου είναι η προμήθεια, εγκατάσταση και λειτουργία ολοκληρωμένης υποδομής κυβερνοασφάλειας, η οποία περιλαμβάνει όλες τις απαιτούμενες υποδομές για Virtualization / OS SW, Data Lake solution, Backup / Data Protection / CyberResiliency / Disaster Recovery solutions, Operations Center Monitoring solutions, Physical Security solutions, Power & Cooling in, Server, Storage, Networking, Cybersecurity SW solutions, AI/ML solutions, integration Services, CTI feeds, κ.λπ. Η εν λόγω προμήθεια θα πραγματοποιηθεί στο πλαίσιο του ευρωπαϊκού έργου EL-SOC, το οποίο υλοποιείται από την Εθνική Αρχή Κυβερνοασφάλειας και συγχρηματοδοτούμενο από το Πρόγραμμα DEP (No 101127713) και το ΑΠΔΕ με κωδικό ΣΑΕ 0632 και κωδικό ενάριθμο έργου 2025ΣΕ063200005.

2. Αντικείμενο του έργου EL-SOC (Enhancing the capacity of the Hellenic Consolidated Security Operation Center) είναι η ενίσχυση της ικανότητας του Ελληνικού Επιχειρησιακού Κέντρου Ενοποιημένης Ασφάλειας, με στόχο τη βελτίωση της εθνικής ασφάλειας στον κυβερνοχώρο, την ανθεκτικότητα με ταχύτερο εντοπισμό και ανταπόκριση σε περιστατικά και απειλές κυβερνοασφάλειας. Συγκεκριμένα, το έργο στοχεύει να αναπτύξει τις δυνατότητες ανίχνευσης και ανάλυσης απειλών στον κυβερνοχώρο, αξιοποιώντας τεχνολογίες αιχμής για να αυξήσουν την επίγνωση της κατάστασης και ενίσχυση των ικανοτήτων σε εθνικό επίπεδο. Η ενίσχυση της λειτουργίας του EL-SOC συνδέεται άμεσα με την υλοποίηση σχετικών πρωτοβουλιών της ΕΕ, όπως:

1. η στρατηγική της ΕΕ για την κυβερνοασφάλεια για τους στόχους της ψηφιακής δεκαετίας,
2. η NIS 2 Οδηγία,
3. ο νόμος για την ασφάλεια στον κυβερνοχώρο,
4. ο κανονισμός ECCC,
5. η σύσταση της Επιτροπής για τη δημιουργία μιας κοινής μονάδας κυβερνοχώρου και
6. το Blueprint για την ασφάλεια στον κυβερνοχώρο, την εργαλειοθήκη ασφάλειας 5G.

Το έργο στοχεύει στην απόκτηση τεχνολογιών και υπηρεσιών που θα αναβαθμίσουν την επιχειρησιακή ικανότητα του EL-SOC στους ακόλουθους τομείς:

i. Συλλογή και επεξεργασία πληροφοριών με χρήση προηγμένης τεχνολογίας εργαλείων
ii. Ανάπτυξη κατάλληλων υποδομών για την αξιοποίηση της κοινής δεξαμενής γνώσης μεταξύ των εθνικών δικτύων SOC (δηλ. μέσω δημιουργίας λίμνης δεδομένων)
iii. Ανάλυση πληροφοριών και εντοπισμό απειλών/επιθέσεων
iv. Δημιουργία αναφορών και κατάλληλων καναλιών ανταλλαγής πληροφοριών
v. Απόκριση περιστατικών
vi. Διαχείριση, ασφάλεια, συντήρηση και λειτουργία της βασικής υποδομής SOC
vii. Βελτιωμένο συντονισμό και συνεργασία των ενδιαφερομένων μερών (π.χ. φορείς εκμετάλλευσης βασικών υπηρεσιών SOC, τομεακές SOCs, το National CSIRT και το CERT) για την ανταπόκριση σε συμβάντα στον κυβερνοχώρο μεταξύ των ενδιαφερομένων.

4. Η εγκατάσταση των συστημάτων θα γίνει εντός κτηρίου της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης (ΓΓΠΣΨΔ), όπου στεγάζεται η Εθνική Αρχή Κυβερνοασφάλειας, σε χώρο εμβαδού- 2.705 τμ περίπου.- Οι οικονομικοί φορείς θα πρέπει να προτείνουν τις τεχνικές προδιαγραφές, συμπεριλαμβανομένων των ποσοτήτων και διαστάσεων, προκειμένου να διασφαλιστεί τόσο η ομαλή εγκατάσταση όσο και η ορθή λειτουργία τους.

5. Οι απαιτήσεις του έργου έχουν κατανεμηθεί σε επιμέρους Λειτουργικές Ενότητες (Lots). Κάθε Lot αποτελεί μια διακριτή τεχνική και λειτουργική ομάδα προμηθειών ή υπηρεσιών, με ειδικές απαιτήσεις, τεχνικά χαρακτηριστικά και όρους συμμόρφωσης. Οι συμμετέχοντες στη διαβούλευση μπορούν να προτείνουν τεχνικές λύσεις που έχουν το ίδιο λειτουργικό αποτέλεσμα με τις παρούσες προκαταρκτικές τεχνικές προδιαγραφές και σε κάθε περίπτωση με τεκμηριωμένες προτάσεις και με αντίστοιχη επισήμανση σε συγκεκριμένους όρους των τεχνικών προδιαγραφών.

2. ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

2.1 Το έργο υποδιαιρείται σε Λειτουργικές Ενότητες (Lots). Για όλα τα υποσυστήματα/τεχνολογικές λύσεις που θα προταθούν, θα πρέπει να συνοδεύονται από:

- αναλυτική παρουσίαση/καταγραφή της πρότασης
- αναλυτική οικονομική προσφορά διάρκειας τριών ετών
- υποστήριξη διάρκειας τριών ετών (updates, upgrades)
- εκπαίδευση προσωπικού της ΕΑΚ στη λειτουργία/χρήση

Παρακάτω αναφέρονται οι προτεινόμενες Λειτουργικές Ενότητες (Lots):

Lot 1 Πλατφόρμα SOC (SIEM/SOAR): [EL-SOC HUB] - [SIEM/SOAR NCSA]

Αφορά την εγκατάσταση, παραμετροποίηση και λειτουργία πλατφόρμας SIEM/SOAR προκειμένου το EL-SOC να μπορεί να αναλάβει διττό ρόλο: ως πάροχος SOC για την Εθνική Αρχή Κυβερνοασφάλειας και ως εθνικό ενοποιημένο SOC-HUB για όλα τα μέλη του «Εθνικού Δικτύου SOC».

Απαιτούνται δυνατότητες συλλογής, διαχείρισης και ανάλυσης δεδομένων, αυτοματοποιημένων playbooks, AI/ML ανίχνευσης, διαλειτουργικότητα με άλλα SIEMs και υποστήριξη για την επιχειρησιακή λειτουργία του SOC.

Ειδικότερα, οι τεχνολογικές λύσεις που θα προταθούν, θα πρέπει να καλύπτουν τα παρακάτω:

- ON-PREMISE solution
- ανεξαρτησία από Services εκτός ΕΑΚ
- δυνατότητα offline update και upgrade
- τεχνική υποστήριξη και συντήρηση από τον ανάδοχο στις εγκαταστάσεις της ΕΑΚ

Λεπτομέρειες και διευκρινήσεις θα μπορούν να δοθούν σε απευθείας επικοινωνία.

Lot 2: Data Center & Δικτυακή Υποδομή

Περιλαμβάνει τη διαμόρφωση και εξοπλισμό του Data Center με racks, καλωδιώσεις, φυσική και περιβαλλοντική ασφάλεια, καθώς και τον απαιτούμενο δικτυακό εξοπλισμό (routers, switches, firewalls, VPN, WAF, NAC κ.ά.) και προστασία επιπέδου δικτύου (π.χ. Anti-DDoS).

Ειδικότερα, οι τεχνολογικές λύσεις που θα προταθούν, θα πρέπει να καλύπτουν τα παρακάτω:

- ON-PREMISE solutions (routers, switches, firewalls, VPN, NAC, antiddos, κτλ)
- αποφυγή εξάρτησης από Services εκτός ΕΑΚ
- τεχνική υποστήριξη και συντήρηση από τον ανάδοχο στις εγκαταστάσεις της ΕΑΚ

Λεπτομέρειες και διευκρινήσεις θα μπορούν να δοθούν σε απευθείας επικοινωνία.

Lot 3 – Αίθουσα Επιχειρήσεων (Operational Room) και Ψηφιακή Υποδομή Παρακολούθησης:

Το Operational Room του EL-SOC έχει σχεδιαστεί για να διευκολύνει απρόσκοπτες και ασφαλείς λειτουργίες κυβερνοασφάλειας μέσω προηγμένων τεχνολογιών και ισχυρών υποδομών.

Περιλαμβάνει τη δημιουργία του επιχειρησιακού χώρου με εξοπλισμό όπως Video Wall, σταθμοί εργασίας, τηλεδιάσκεψη, VoIP, πολυμηχανήματα και πλήρη δομημένη καλωδίωση για τη διασύνδεση όλων των συστημάτων.

Ειδικότερα, οι τεχνολογικές λύσεις που θα προταθούν, θα πρέπει να καλύπτουν τα παρακάτω:

- αποφυγή εξάρτησης από Services εκτός ΕΑΚ
- τεχνική υποστήριξη και συντήρηση από τον ανάδοχο στις εγκαταστάσεις της ΕΑΚ

Λεπτομέρειες και διευκρινήσεις θα μπορούν να δοθούν σε απευθείας επικοινωνία.

Lot 4 – Πληροφοριακά Συστήματα & Εικονικοποίηση:

Περιλαμβάνει την προμήθεια και εγκατάσταση της υπολογιστικής και αποθηκευτικής υποδομής (servers, storage), πλατφόρμα virtualization, backup λύση on-premise και υπηρεσίες πληροφορικής όπως domain controller και email/DNS protection.

Ειδικότερα, οι τεχνολογικές λύσεις που θα προταθούν, θα πρέπει να καλύπτουν τα παρακάτω:

- αποφυγή εξάρτησης από Services εκτός ΕΑΚ
- τεχνική υποστήριξη και συντήρηση από τον ανάδοχο στις εγκαταστάσεις της ΕΑΚ

Λεπτομέρειες και διευκρινήσεις θα μπορούν να δοθούν σε απευθείας επικοινωνία.

Lot 5 – Πλατφόρμα Τεχνητής Νοημοσύνης (AI Platform), Πλατφόρμες Cyber Threat Intelligence και Εργαλεία Ανάλυσης (Forensic Tools):

Αφορά την υλοποίηση ON-PREM πλατφόρμας AI με δυνατότητα λειτουργίας πολλαπλών LLMs με διασύνδεση με το SOC, CTI πλατφόρμες (με IoC search, MITRE mapping και threat actor intelligence, κτλ) καθώς εργαλεία ανάλυσης ψηφιακών ιχνών (forensic tools).

Ειδικότερα, οι τεχνολογική λύση για την Πλατφόρμα Τεχνητής Νοημοσύνης (AI Platform) που θα προταθεί, θα πρέπει να καλύπτει τα παρακάτω:

- ON-PREMISE solution (δυνατότητα air-gap λειτουργίας)
- ανεξαρτησία από Services εκτός ΕΑΚ
- δυνατότητα offline update και upgrade
- τεχνική υποστήριξη και συντήρηση από τον ανάδοχο στις εγκαταστάσεις της ΕΑΚ

Λεπτομέρειες και διευκρινήσεις θα μπορούν να δοθούν σε απευθείας επικοινωνία.

2. Είναι πιθανό ορισμένα Lots να παρουσιάζουν τεχνική ή χρονική αλληλεξάρτηση μεταξύ τους, υπό την έννοια ότι η υλοποίηση ή η ορθή λειτουργία ενός Lot ενδέχεται να προϋποθέτει την ολοκλήρωση ή τη διαθεσιμότητα ενός άλλου. Οι ενδιαφερόμενοι οικονομικοί φορείς καλούνται να λάβουν υπόψη αυτές τις ενδεχόμενες αλληλεξαρτήσεις, να τις επισημαίνουν στην τεχνική τους λύση και να προτείνουν τις αντίστοιχες πρόσφορες τεχνικές προδιαγραφές.

Ακολουθούν τα προτεινόμενα Lots (Lot 1, 2, 3, 4 και 5) με στόχο την παροχή επαρκούς τεχνικής πληροφόρησης προς την αγορά**.**

Πίνακας Τεχνικών Προδιαγραφών

LOT 1.1: Πλατφόρμα για [EL-SOC HUB]

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ EL-SOC HUB
1.1	**Γενική Περιγραφή**	• Εγκατάσταση και διαμόρφωση της πλατφόρμας EL-SOC ως National HUB, με πλήρη δυνατότητα συλλογής, ανάλυσης και απόκρισης σε κυβερνοαπειλές και δυνατότητα διασύνδεσης με όλα τα γνωστά SIEMs/SOARs. • Δυνατότητα λειτουργίας σε air-gapped περιβάλλοντα. • Η υποδομή θα πρέπει να περιλαμβάνει ισχυρές δυνατότητες επεξεργασίας δεδομένων. Ο Ρυθμός συλλογής των δεδομένων καταγραφής από τα υπό παρακολούθηση συστήματα θα πρέπει να αναφερθεί. • Η πλατφόρμα θα εγκατασταθεί και θα λειτουργεί στις εγκαταστάσεις της Εθνικής Αρχής Κυβερνοασφάλειας
1.2	**Εγκατάσταση και λειτουργία πλατφόρμας στις εγκαταστάσεις της ΕΑΚ**	• Η πλατφόρμα θα εγκατασταθεί και θα λειτουργεί στις εγκαταστάσεις της ΕΑΚ με τη δυνατότητα οι ενημερώσεις (updates) και οι αναβαθμίσεις (upgrades) να μπορούν να γίνονται OFFLINE. • Δεν θα υπάρχει απευθείας σύνδεση της πλατφόρμας με τον κατασκευαστή. • Δυνατότητα μελλοντικής αναβάθμισης τόσο στο λογισμικό (software) όσο και στο υλικό (hardware) τα οποία θα συνοδεύονται με 3ετή τουλάχιστον εγγύηση από την ημερομηνία υπογραφής της σχετικής σύμβασης.
1.3	**Δυνατότητα multi-tenancy**	• Δυνατότητα **multi-tenancy** • Δυνατότητα ομαδοποίησης οργανισμών (tenants) σε κατηγορίες
1.4	**Συλλογή δεδομένων από τουλάχιστον 300+ πηγές (logs/events)**	• Η πλατφόρμα να έχει δυνατότητα λήψης, επεξεργασίας και ομαδοποίησης logs/events/offences/incidents από πολλαπλές πηγές.

		• Να υποστηρίζεται η συλλογή από πάνω από 300 πηγές με δυνατότητα normalization & parsing. • Ο ρυθμός συλλογής δεδομένων θα πρέπει να αναφερθεί.
1.5	**Playbooks και Απόκριση σε περιστατικά**	• Δημιουργία σε συνεργασία με την Αναθέτουσα Αρχή τουλάχιστον 10 playbooks με παραμετροποίηση και σενάρια αυτοματοποίησης ενεργειών. • Εκπαίδευση προσωπικού ΕΑΚ στη δημιουργία και παραμετροποίηση αυτών.
1.6	**Δυνατότητα διασύνδεσης με όλα τα γνωστά SIEMs/SOARs**	• Η πλατφόρμα να έχει τη δυνατότητα διασύνδεσης με εξωτερικά SIEMs διαφορετικών κατασκευαστών. • Υποστήριξη πλήρως μέσω connectors/API integrations και προηγούμενης εμπειρίας.
1.7	**Διασύνδεση και παραμετροποίηση της πλατφόρμας με τουλάχιστον 10 SIEM λύσεις**	• Παραμετροποίηση της πλατφόρμας και διασύνδεση με τουλάχιστον 10 SIEM/SOAR λύσεις. • Εκπαίδευση προσωπικού ΕΑΚ στη διασύνδεση και παραμετροποίηση της πλατφόρμας με SIEM/SOAR λύσεις.
1.8	**UEBA & AI/ML Δυνατότητες**	• Η πλατφόρμα να περιλαμβάνει δυνατότητες μηχανικής μάθησης και ανάλυσης συμπεριφοράς (User/Entity Behavior Analytics). Υποστήριξη μέσω ενσωματωμένων μηχανών ανάλυσης κινδύνου και μοντέλων τεχνητής νοημοσύνης (AI). • Η όλη επεξεργασία των πληροφοριών από το υποσύστημα τεχνητής νοημοσύνης (AI) να γίνεται στις εγκαταστάσεις της Αναθέτουσας Αρχής, χωρίς καμία εξωτερική επικοινωνία. • Τα αποτελέσματα ανάλυσης της τεχνητής νοημοσύνης να παρουσιάζονται στον Αναλυτή της Αναθέτουσας Αρχής με απλό και κατανοητό τρόπο, ώστε να μπορεί να καθοδηγηθεί στα επόμενα βήματα.
1.9	**Δεδομένα καταγραφής**	• Η πλατφόρμα θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων καταγραφής κατά την αποστολή τους προς αυτήν. • Να υπάρχει πιστοποίηση της ασφαλούς αποθήκευσης σε σύστημα αποθήκευσης μετά την επεξεργασία τους.

		• Εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής χρησιμοποιώντας τεχνικές μεγάλων δεδομένων (big data) και ελαστικότητας (elasticity). • Η πλατφόρμα να δίνει την δυνατότητα παραγωγής σχετικών αναφορών με εφαρμογή ειδικών φίλτρων. • Εφαρμογή κανόνων συσχέτισης (correlation rules) σε πραγματικό χρόνο καθώς τα δεδομένα εισέρχονται στο κεντρικό σύστημα επεξεργασίας. • Η πλατφόρμα ασφαλείας να εκμεταλλεύεται/ χρησιμοποιεί την συσχέτιση από διαφορετικές πηγές (συστήματα και εφαρμογές).
1.10	**Alerts**	• Δημιουργία και αποστολή ειδοποιήσεων (alerts) σε καθορισμένους χρήστες με χρήση ηλεκτρονικού ταχυδρομείου (email). • Παραγωγή alerts με βάση τη συχνότητα και τον χρόνο εμφάνισης κάποιου γεγονότος, καθώς επίσης και όταν κάποιος κανόνας πληρείται. • Δυνατότητα ιεράρχησης της υπό παρακολούθηση υποδομής βάσει των ιδιαίτερων χαρακτηριστικών των συστημάτων και εφαρμογών καθώς και της χρησιμοποίησης αυτών στην δημιουργία κανόνων συσχέτισης. • Τα χαρακτηριστικά αυτά θα μπορούν να καθορίζουν την κρισιμότητα και κατηγοριοποίηση των παραγόμενων ειδοποιήσεων (alerts). • Παραγωγή ειδοποίησης (alert) όταν κάποια πηγή (πχ logs source, event source) σταματήσει να στέλνει δεδομένα για ορισμένο χρονικό διάστημα. Το χρονικό διάστημα θα εξαρτάται από τον τύπο της συσκευής και την σπουδαιότητα αυτής στην παρεχόμενη πλατφόρμα ασφαλείας, και θα είναι παραμετροποιήσιμο. • Δημιουργία αναφορών προσαρμοσμένων στις απαιτήσεις και ανάγκες του χρήστη (custom reports) χρησιμοποιώντας ως παράμετρο κάθε είδους πληροφορία η οποία περιέχεται στα δεδομένα καταγραφής
1.11	**GDPR Συμμόρφωση**	• Η πλατφόρμα να είναι συμβατή με τις απαιτήσεις του GDPR. Η λύση θα πρέπει να πλήρως

		συμμορφούμενη με τον GDPR και να υποστηρίζει auditing/logging**.**

LOT 1. 2: Πλατφόρμα για [SIEM/SOAR NCSA]

Α/Α	**ΠΡΟΔΙΑΓΡΑΦΗ**	**ΑΠΑΙΤΗΣΗ** **SIEM/SOAR NCSA**
1.1	**Γενική Περιγραφή**	• Εγκατάσταση και διαμόρφωση της πλατφόρμας EL-SOC ως SOC (SIEM/SOAR) της Εθνικής Αρχής Κυβερνοασφάλειας, με πλήρη δυνατότητα συλλογής, ανάλυσης και απόκρισης σε κυβερνοαπειλές. • Η υποδομή θα πρέπει να περιλαμβάνει ισχυρές δυνατότητες επεξεργασίας δεδομένων. Ο Ρυθμός συλλογής των δεδομένων καταγραφής από τα υπό παρακολούθηση συστήματα θα πρέπει να αναφερθεί. • Η πλατφόρμα θα εγκατασταθεί και θα λειτουργεί στις εγκαταστάσεις της Εθνικής Αρχής Κυβερνοασφάλειας.
1.2	**Εγκατάσταση και λειτουργία πλατφόρμας στις εγκαταστάσεις της ΕΑΚ**	• Η πλατφόρμα θα εγκατασταθεί και θα λειτουργεί στις εγκαταστάσεις της ΕΑΚ με τη δυνατότητα οι ενημερώσεις (updates) και οι αναβαθμίσεις (upgrades) να μπορούν να γίνονται offline. • Δεν θα υπάρχει απευθείας σύνδεση της πλατφόρμας με τον κατασκευαστή. • Δυνατότητα μελλοντικής αναβάθμισης τόσο στο λογισμικό (software) όσο και στο υλικό (hardware) τα οποία θα συνοδεύονται με 3ετή τουλάχιστον εγγύηση από την ημερομηνία υπογραφής της σχετικής σύμβασης.
1.3	**Δυνατότητα multi-tenancy**	• Δυνατότητα multi-tenancy • Δυνατότητα ομαδοποίησης οργανισμών (tenants) σε κατηγορίες
1.4	**Πηγές Εισόδου**	• Υποστήριξη για τουλάχιστον 500 πηγές εισόδου (logs, netflow, κτλ). • Να αναφερθούν αναλυτικά οι απαιτήσεις σε εξοπλισμό.
1.5	**Playbooks και Απόκριση σε περιστατικά**	• Δημιουργία σε συνεργασία με την Αναθέτουσα Αρχή τουλάχιστον 10 playbooks με παραμετροποίηση και σενάρια αυτοματοποίησης ενεργειών.

		• Εκπαίδευση προσωπικού ΕΑΚ στη δημιουργία και παραμετροποίηση αυτών.
1.6	**UEBA & AI/ML Δυνατότητες**	• Η πλατφόρμα να περιλαμβάνει δυνατότητες μηχανικής μάθησης και ανάλυσης συμπεριφοράς (User/Entity Behavior Analytics). Υποστήριξη μέσω ενσωματωμένων μηχανών ανάλυσης κινδύνου και μοντέλων AI. • Η όλη επεξεργασία των πληροφοριών από το υποσύστημα τεχνητής νοημοσύνης (AI) να γίνεται στις εγκαταστάσεις της Αναθέτουσας Αρχής, χωρίς καμία εξωτερική επικοινωνία. • Τα αποτελέσματα ανάλυσης της τεχνητής νοημοσύνης να παρουσιάζονται στον Αναλυτή της Αναθέτουσας Αρχής με απλό και κατανοητό τρόπο, ώστε να μπορεί να καθοδηγηθεί στα επόμενα βήματα.
1.7	**Δεδομένα καταγραφής**	• Άντληση δεδομένων καταγραφής ή δικτυακών ροών ή κίνησης δικτύου (κατά απαίτηση) από κάθε πληροφοριακό σύστημα ή εφαρμογή της υποδομής, ανεξαρτήτως κατασκευαστή, το οποίο θα κριθεί πως θα πρέπει να συμμετέχει στην πλατφόρμα όπως: ○ Συστήματα ασφάλειας (Firewalls, IDS/IPS, Content Security systems, VPNs, Vulnerability scanners, Antivirus servers, AAA servers, NAC κ.α.) ○ Συσκευές Δικτύου (Routers, Switches) ○ Λειτουργικά Συστήματα ○ Βάσεις Δεδομένων, Directory Services, Web Servers, ○ Applications • Η πλατφόρμα θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων καταγραφής κατά την αποστολή τους προς αυτήν. • Να υπάρχει πιστοποίηση της ασφαλούς αποθήκευσης σε σύστημα αποθήκευσης μετά την επεξεργασία τους. • Εύκολη και γρήγορη αναζήτηση ανάμεσα στα αποθηκευμένα δεδομένα καταγραφής χρησιμοποιώντας τεχνικές μεγάλων δεδομένων (big data) και ελαστικότητας (elasticity).

		• Η πλατφόρμα να δίνει την δυνατότητα παραγωγής σχετικών αναφορών με εφαρμογή ειδικών φίλτρων. • Εφαρμογή κανόνων συσχέτισης (correlation rules) σε πραγματικό χρόνο καθώς τα δεδομένα εισέρχονται στο κεντρικό σύστημα επεξεργασίας. • Η πλατφόρμα ασφαλείας να εκμεταλλεύεται/ χρησιμοποιεί την συσχέτιση από διαφορετικές πηγές (συστήματα και εφαρμογές).
1.8	**Alerts**	• Δημιουργία και αποστολή ειδοποιήσεων (alerts) σε καθορισμένους χρήστες με χρήση ηλεκτρονικού ταχυδρομείου (email). • Παραγωγή alerts με βάση τη συχνότητα και τον χρόνο εμφάνισης κάποιου γεγονότος, καθώς επίσης και όταν κάποιος κανόνας πληρείται. • Δυνατότητα ιεράρχησης της υπό παρακολούθηση υποδομής βάσει των ιδιαίτερων χαρακτηριστικών των συστημάτων και εφαρμογών καθώς και της χρησιμοποίησης αυτών στην δημιουργία κανόνων συσχέτισης. • Τα χαρακτηριστικά αυτά θα μπορούν να καθορίζουν την κρισιμότητα και κατηγοριοποίηση των παραγόμενων ειδοποιήσεων (alerts). • Παραγωγή ειδοποίησης (alert) όταν κάποια πηγή (πχ logs source, event source) σταματήσει να στέλνει δεδομένα για ορισμένο χρονικό διάστημα. Το χρονικό διάστημα θα εξαρτάται από τον τύπο της συσκευής και την σπουδαιότητα αυτής στην παρεχόμενη πλατφόρμα ασφαλείας, και θα είναι παραμετροποιήσιμο. • Δημιουργία αναφορών προσαρμοσμένων στις απαιτήσεις και ανάγκες του χρήστη (custom reports) χρησιμοποιώντας ως παράμετρο κάθε είδους πληροφορία η οποία περιέχεται στα δεδομένα καταγραφής
1.9	**GDPR Συμμόρφωση**	• Η πλατφόρμα να είναι συμβατή με τις απαιτήσεις του GDPR. Η λύση θα πρέπει να πλήρως συμμορφούμενη με τον GDPR και να υποστηρίζει auditing/logging.

Πίνακας Τεχνικών Προδιαγραφών
LOT 2: Data Center & Δικτυακή Υποδομή

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ
2.1	**Γενική Περιγραφή**	Το Lot περιλαμβάνει την πλήρη υλοποίηση φυσικής και δικτυακής υποδομής για το EL-SOC, συμπεριλαμβανομένων των Data Center racks, καλωδιώσεων, εξοπλισμού ασφαλείας και βασικού cybersecurity stack. Η προτεινόμενη λύση να καλύπτει πλήρως τις απαιτήσεις μέσω ON-PREM εγκατάστασης με πλήρη ελέγξιμη λειτουργία.
2.2	**Εγκατάσταση έως 8 ικριωμάτων (racks) στο Data Center**	• Υποστήριξη έως και 8 ικριωμάτων racks για ολόκληρο τον μηχανογραφικό και δικτυακό εξοπλισμό. • Παροχή πλήρους λύσεως εγκατάστασης των ικριωμάτων και συναφούς υποδομής.

2.3	**Συστήματα φυσικής ασφάλειας**	• Εγκατάσταση πλήρους κλειστού συστήματος τηλεόρασης-CCTV (ανεξάρτητο σύστημα) για την επιτήρηση χώρων του του data center, και του Operational Room.
		  ○ Το CCTV να έχει δυνατότητα offline ενημερώσεων (updates)και αναβαθμίσεων (upgrades).
		  ○ Το σύστημα θα έχει την δυνατότητα παρακολούθησης των καμερών σε πραγματικό χρόνο, αναζήτησης αποθηκευμένου video με κριτήρια όπως κάμερα, ώρα, ημέρα κλπ.
		  ○ Η ωφέλιμη χωρητικότητα για την καταγραφή video θα είναι τουλάχιστον για 15 ημέρες
		• Εγκατάσταση Συστήματος ελέγχου πρόσβασης (μονάδες ανάγνωσης καρτών με ενσωματωμένο πληκτρολόγιο, τοποθέτηση καρταναγνώστη στην είσοδο/έξοδο του χώρου.
		  ○ Ο Ανάδοχος να προσφέρει και σχετική μονάδα προγραμματισμού καρτών
		  ○ Το σύστημα να έχει τη δυνατότητα να προγραμματίζει διαφορετικά προφίλ πρόσβασης
		  ○ Το σύστημα να ενεργοποιεί συναγερμό (με ηχητικό σήμα σε περίπτωση παραβίασης της θύρας)
		• Τα Συστήματα φυσικής ασφάλειας, θα πρέπει να λειτουργούν χωρίς διασύνδεση στο Internet.
		• Η διαχείρισή τους θα γίνεται από το τοπικό εσωτερικό δίκτυο.

2.4	**Δικτυακός εξοπλισμός (Routers, Switches, Firewalls, VPN, Data Diodes)**	• Πλήρης κάλυψη των δικτυακών αναγκών του SOC, με έμφαση στη διαθεσιμότητα και ασφάλεια. • Σύγχρονος, διαχειρίσιμος εξοπλισμός με δυνατότητα VLANs και πολλαπλές ζώνες ασφαλείας • Η VPN λύση να εξυπηρετεί τις όλες ανάγκες διασύνδεσης του EL-SOC (HUB και SIEM/SOAR NCSA**)** • Hardware Data Diodes
2.5	**Υποστήριξη Anti-DDoS, WAF και έλεγχος πρόσβασης δικτύου (NAC)**	• ON-PREM λύσεις για προστασία από επιθέσεις δικτύου (DDoS και WAF), και έλεγχος πρόσβασης (NAC)
2.6	**Συμβατότητα με διεθνή πρότυπα TIER 3**	• Το Data Center να πληροί τις απαιτήσεις TIER 3 και η υποδομή του να σχεδιαστεί με τρόπο που να ευθυγραμμίζεται με τα διεθνή πρότυπα αξιοπιστίας (πχ TIA-942/EN 50600)
2.7	**DCIM (Data Center Infrastructure Monitoring)**	• Παρακολούθηση κρίσιμων παραμέτρων του εξοπλισμού (θερμοκρασία, υγρασία, ρεύματος και συναγερμών. • Οι λύσεις θα πρέπει να παρέχουν τη δυνατότητα για αποστολή ειδοποιήσεων για οποιοδήποτε σφάλμα ή παρατυπία.
2.8	**Αδιάλειπτη παροχή ισχύος (UPS)**	• Το σύστημα να βασίζεται σε υπάρχουσα υποδομή UPS με δυνατότητα ενσωμάτωσης. Κρίνεται απαραίτητη η διασφάλιση της συμβατότητας σύμφωνα με τις υπάρχουσες υποδομές UPS.
2.9	**Ασφάλεια καλωδιώσεων & access points**	• Όλα τα καλώδια να είναι οργανωμένα και πιστοποιημένα (πχ EN 50173 / ISO 11801) χωρίς έκθεση ή ανεξέλεγκτη πρόσβαση. • Πλήρης διαχείριση και καταγραφή καλωδιώσεων με χρήση patch panels και πιστοποιημένων συνδέσεων.
2.10	**Καλωδίωση από υπόγειο σε ορόφους 1 & 2 και διαφοροποίηση ανά τύπο δικτύου**	• Να υλοποιηθεί κατακόρυφη και οριζόντια καλωδίωση από τον χώρο του data center σε ορόφους. • Να χρησιμοποιούνται διαφορετικοί τύποι καλωδίων για διαφορετικά δίκτυα (π.χ. management, data, voice). • Όλα τα καλώδια θα πρέπει να είναι σημασμένα και πιστοποιημένα (πχ EN 50173 / ISO 11801)

Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης

Πίνακας Τεχνικών Προδιαγραφών
LOT 3: Operational Room & Ψηφιακή Υποδομή Παρακολούθησης

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ
3.1	**Γενική Περιγραφή**	Το Lot περιλαμβάνει την προμήθεια και εγκατάσταση εξοπλισμού και τεχνολογιών για την αίθουσα επιχειρήσεων (Operational Room-OR) του EL-SOC. Το OR θα πρέπει να διευκολύνει απρόσκοπτες και ασφαλείς λειτουργίες κυβερνοασφάλειας μέσω προηγμένων τεχνολογιών και ισχυρών υποδομών. Οι λύσεις θα πρέπει να καλύπτουν πλήρως τις απαιτήσεις για λειτουργικότητα, οπτικοποίηση, συνεργασία και ασφάλεια στον χώρο επιχειρήσεων.
3.2	**Σύστημα ελέγχου πρόσβασης**	• Αυτόνομο σύστημα ελέγχου πρόσβασης που θα περιλαμβάνει: κομβίο κουδουνιού για επισκέπτες, δυνατότητα καταγραφής εισόδου/εξόδου, δυνατότητα απομακρυσμένης διαχείρισης του συστήματος εντός του εσωτερικού δικτύου (χωρίς πρόσβαση στο διαδίκτυο) • Να υπάρχει δυνατότητα κατά περίπτωση προγραμματισμού για επισκέπτες
3.3	**Video Wall και Wall Controller**	• Σύστημα προβολής LED video wall διαστάσεων 7x2 μ. με controller και λογισμικό διαχείρισης εικόνας. • Εγκατάσταση video wall υψηλής ανάλυσης και ελέγχου από ανεξάρτητο σταθμό εργασίας. • Διαχείριση του video wall και του video wall controller από ανεξάρτητο σύστημα αυτοματισμού για τον έλεγχο του συστήματος μέσω ενός σταθμού εργασίας τοπικού δικτύου.
3.4	**Σταθμοί Εργασίας**	• 10 σταθμοί εργασίας με πλήρη περιφερειακά (οθόνες, πληκτρολόγια, mouse, headsets).

		• Η λύση να περιλαμβάνει παραμετροποιήσιμο hardware με πιστοποίηση CE και εργονομικά εξαρτήματα.
3.5	**Τηλεδιάσκεψη & VoIP**	• Πλήρες Σύστημα τηλεδιάσκεψης και συσκευές VoIP με air-gapped λειτουργία. • Προβλέπεται ανεξάρτητη εγκατάσταση με διασύνδεση εντός εσωτερικού δικτύου μόνο.
3.6	**Πολυμηχανήματα**	•3 δικτυακά έγχρωμα πολυμηχανήματα με σάρωση διπλής όψης και αποστολή σε Η/Υ. • Συμπεριλαμβάνονται συσκευές με αντίστοιχες δυνατότητες και προεγκατεστημένα τόνερ.
3.7	**Δομημένη Καλωδίωση**	• Καλωδίωση με τερματισμούς σε patch-panels και τήρηση προτύπων EN 50173 / ISO 11801. • Η προσφερόμενη λύση περιλαμβάνει πλήρη χαρτογράφηση και πιστοποίηση καλωδίωσης.

Πίνακας Τεχνικών Προδιαγραφών
LOT 4: Πληροφοριακά Συστήματα & Εικονικοποίηση

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ
4.1	**Γενική Περιγραφή**	• Το Lot αφορά την εγκατάσταση και παραμετροποίηση της υπολογιστικής υποδομής, περιλαμβάνοντας virtualization, αποθήκευση και βασικές υπηρεσίες πληροφορικής. • Οι προτεινόμενες λύσεις να βασίζονται σε αξιόπιστους κατασκευαστές και τεχνολογίες enterprise-grade. • Η τεχνολογική λύση θα εγκατασταθεί και θα λειτουργεί (OnPrem Solution) στο Data Center της Εθνικής Αρχής Κυβερνοασφάλειας με πλήρη ελέγξιμη λειτουργία.
4.2	**Virtualization Platform & Licenses**	• Παροχή λογισμικού virtualization (hypervisor) με αντίστοιχες άδειες και εργαλείο διαχείρισης. • Χρήση πλατφόρμας virtualization ευρείας αποδοχής
4.3	**Storage & High Availability**	• Υποδομή αποθήκευσης με υποστήριξη HA και δυνατότητα αποθήκευσης logs/events. • Προβλέπεται διαμοιρασμένο storage με redundancy και δυνατότητα επέκτασης.
4.4	**Domain Controller και Active Directory**	• Υπηρεσίες ελεγκτή τομέα με Active Directory και λογισμικό διαχείρισης χρηστών/πολιτικών. • Η λύση να περιλαμβάνει πλήρες περιβάλλον AD για εσωτερική διαχείριση ταυτοποίησης.
4.5	**Backup Infrastructure (VMs & Data)**	• Λύση on-premise backup με δυνατότητα προστασίας VMs και δεδομένων. • Προβλέπεται υλοποίηση air-gapped backup με ισοδύναμα μέσα αποθήκευσης και επαναφοράς.
4.6	**Email & DNS Protection**	• Να περιλαμβάνονται μηχανισμοί προστασίας email και DNS εντός της υποδομής. • Στην προσφερόμενη λύση περιλαμβάνονται υπηρεσίες filtering και παρακολούθησης.

Πίνακας Τεχνικών Προδιαγραφών

LOT 5: Πλατφόρμα Τεχνητής Νοημοσύνης (AI Platform), Πλατφόρμες Cyber Threat Intelligence και Εργαλεία Ανάλυσης (Forensic Tools)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ
5.1	**Γενική Περιγραφή**	Το Lot περιλαμβάνει την προμήθεια και εγκατάσταση Πλατφόρμας Τεχνητής Νοημοσύνης και λύσεων Cyber Threat Intelligence (CTI) καθώς και forensic εργαλείων για την ενίσχυση των δυνατοτήτων ανάλυσης, πρόβλεψης και αντίδρασης σε απειλές. Η προσφερόμενη λύση για την Πλατφόρμα Τεχνητής Νοημοσύνης , να καλύπτει πλήρως τις απαιτήσεις ON-PREM εγκατάστασης των LLMs. Για τις Πλατφόρμες Cyber Threat Intelligence να αναφερθούν αναλυτικά για την κάθε προτεινόμενη λύση: • οι δυνατότητες αναζήτησης • η πλήρης λίστα των διαθέσιμων παραμέτρων αναζήτησης • η περιγραφή της διαθέσιμης πληροφορίας • οι τύποι παρεχόμενων αναφορών • οι πηγές πληροφόρησης για threat actors και malware intelligence Τα Forensic Tools θα χρησιμοποιηθούν στη διερεύνηση και τεκμηρίωση της ανάλυσης κυβερνοεπιθέσεων.
5.2	**AI Platform: Multi-Agent Αρχιτεκτονική & LLMs**	• Το σύστημα πρέπει να υποστηρίζει πολλαπλούς βοηθούς AI και ταυτόχρονη χρήση διαφορετικών LLMs σε on-premise περιβάλλον. • Υποστήριξη πλήρως μέσω επεκτάσιμης αρχιτεκτονικής με δυνατότητα ενσωμάτωσης custom agents. • Το σύστημα πρέπει να καταγράφει αναλυτικά όλες τις αλληλεπιδράσεις, τις εντολές των χρηστών, τις αποκρίσεις των βοηθών και τη χρήση εργαλείων, διασφαλίζοντας πλήρη ιχνηλασιμότητα και συμμόρφωση με κανόνες διακυβέρνησης δεδομένων.
5.3	**AI Platform: Ενοποίηση με SOC και IT υποδομές**	• Το σύστημα AI να υποστηρίζει διασύνδεση με τα SOC εργαλεία και πληροφοριακές υποδομές.

		• Υλοποίηση με API connectors και εσωτερική αλληλεπίδραση βάσει ρόλων και πολιτικών πρόσβασης.
5.4	**Cyber Threat Intelligence Platforms**	• Ενδεικτικές δυνατότητες πλατφορμών CTI: o Να υποστηρίζουν αναζητήσεις με: IoC, threat actor profiles, MITRE ATT&CK mapping, vulnerabilities. o Να διαθέτουν πρόσβαση με UI και API o Να υποστηρίζουν ιστορικότητα 12+ μηνών. o Να παρέχει αντιστοίχιση των καταγεγραμμένων adversary TTPs στο MITRE ATT&CK framework o Να παρέχει μια βάση δεδομένων vulnerabilities που αξιοποιεί πληροφορίες από open-source vendor advisories, security blogs, και exploit databases. o Να παρέχει παραμετροποιήσιμα reports
5.5	**Forensic Tools**	• Να παρέχονται εργαλεία ανάλυσης ψηφιακών ιχνών και υποστήριξη forensics διεργασιών. Συμπεριλαμβάνονται εργαλεία για συλλογή, επεξεργασία και τεκμηρίωση αποδεικτικών στοιχείων. • Οι λύσεις που θα προταθούν θα πρέπει να αναφέρουν τις αναλυτικές τους προδιαγραφές.
5.6	**Ασφάλεια, Ιχνηλασιμότητα και GDPR**	• Όλα τα δεδομένα και οι διεργασίες AI να είναι πλήρως ON-PREM, με audit logs και συμβατότητα με GDPR. • Η αρχιτεκτονική σχεδιάζεται ώστε να διασφαλίζει πλήρη τοπική λειτουργία και καταγραφή χρήσης.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΠΡΟΚΑΤΑΡΚΤΙΚΗ ΔΙΑΒΟΥΛΕΥΣΗ

Σχέδιο τεχνικών προδιαγραφών για την προμήθεια εγκατάσταση και λειτουργία ολοκληρωμένης υποδομής κυβερνοασφάλειας για τις ανάγκες του έργου DEP: Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC), συγχρηματοδοτούμενο από το Πρόγραμμα DEP (No 101127713), με κωδικό ΣΑΕ 0632 και κωδικό ενάριθμο έργου 2025ΣΕ063200005.

ΕΓΓΡΑΦΟ ΥΠΟΒΟΛΗΣ ΠΡΟΤΑΣΕΩΝ ΚΑΙ ΠΑΡΑΤΗΡΗΣΕΩΝ

Το παρόν έγγραφο προορίζεται για την καταγραφή σχολίων, παρατηρήσεων και τεκμηριωμένων προτάσεων των ενδιαφερόμενων οικονομικών φορέων επί των τεχνικών προδιαγραφών της προμήθειας.

Οι προτάσεις και οι παρατηρήσεις θα διαβιβάζονται στην παρακάτω ηλεκτρονική διεύθυνση της Εθνικής Αρχής Κυβερνοασφάλειας με την χρήση του παρόντος εγγράφου:

Όνομα Υπεύθυνου: .....

Email: .....

Τηλ.: .....

ΠΡΟΤΑΣΕΙΣ ΚΑΙ ΠΑΡΑΤΗΡΗΣΕΙΣ

Όνομα Οικονομικού Φορέα: .....

1. **Γενικές Παρατηρήσεις**

   .....

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

2. Παρατηρήσεις επί των τεχνικών προδιαγραφών

Α/Α	Α/Α LOT	Α/Α ΠΡΟΔΙΑΓΡΑΦΗΣ	ΓΕΝΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ	ΣΕΛΙΔΑ	ΣΧΟΛΙΑ / ΠΡΟΤΑΣΕΙΣ
1					
2					
3					

Ο πίνακας μπορεί να επεκταθεί αναλόγως του αριθμού σχολίων.