**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ**
**ΔΗΜΟΣ ΧΕΡΣΟΝΗΣΟΥ**
**Δ/ΝΣΗ ΔΙΟΙΚΗΤΙΚΩΝ ΥΠΗΡΕΣΙΩΝ**

**Αρ. Μελέτης: ΔΔΥ 03/2023**

**ΚΑ: 10.6112.0001**
**00.6117.0003**
**CPV: 48732000-8**
**79417000-0**

**Ακριβές αντίγραφο**

**Ο Διευθυντής Οικονομικών Υπηρεσιών**

CHARALAMPOS KOUTOULAS
14/06/2023 10:59

**Χαράλαμπος Κούτουλας**

**ΤΙΤΛΟΣ ΜΕΛΕΤΗΣ**

# « ΑΝΑΝΕΩΣΗ, ΣΥΝΤΗΡΗΣΗ, ΑΝΑΒΑΘΜΙΣΗ ΣΥΣΤΗΜΑΤΟΣ ΚΥΒΕΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΕΠΙΤΗΡΗΣΗΣ/ΑΝΑΝΕΩΣΗΣ ΠΙΣΤΟΠΟΙΗΣΕΩΝ ΚΑΤΑ ISO 27001 ΚΑΙ ISO 27701 ΤΟΥ ΔΗΜΟΥ ΧΕΡΣΟΝΗΣΟΥ»

**ΓΟΥΡΝΕΣ, 2023**

**Πίνακας περιεχομένων**

**1. Αναγκαιότητα υλοποίησης της υπηρεσίας**

Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και όχι μόνο. Οι Δήμοι καλούνται να διαχειριστούνε και να προστατέψουνε και άλλης φύσεως δεδομένα όπως Συμβάσεις Έργων, Οικονομικά δεδομένα αλλά και λειτουργείες όπως διαχείριση φωτισμού, ενεργειακών εγκαταστάσεων κ.τ.λ. Η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Οι εξελίξεις αυτές απαιτούν ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων στα κράτη - μέλη της ΕΕ, υποστηριζόμενο από αυστηρή εφαρμογή της νομοθεσίας, δεδομένου ότι είναι σημαντικό να δημιουργηθεί η αναγκαία εμπιστοσύνη που θα επιτρέψει στην ψηφιακή οικονομία να αναπτυχθεί στο σύνολο της εσωτερικής αγοράς.

Καθώς στη σύγχρονη εποχή οι πολίτες όσο και οι φορείς εξαρτώνται όλο και περισσότερο από τα συστήματα επικοινωνιών και πληροφορικής, η ασφάλειά τους αποτελεί πλέον μείζον θέμα εθνικού ενδιαφέροντος, ενώ ταυτόχρονα παρατηρείται μία συνεχώς αυξανόμενη ανάγκη για προστασία των χρηστών ψηφιακών υπηρεσιών και ιδίως νεαρής ηλικίας.

Ο όρος “κυβερνοασφάλεια” αναφέρεται σε όλες εκείνες τις δράσεις και τις ενέργειες που πρέπει να γίνουν, προκειμένου να διασφαλιστεί η προστασία του εκάστοτε φορέα από απειλές.

Η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί εργαλείο για τη βελτίωση της διαδικτυακής ασφάλειας, εξασφαλίζοντας την ακεραιότητα, διαθεσιμότητα και ανθεκτικότητα των κρίσιμων υποδομών και την εμπιστευτικότητα της διακινούμενης ψηφιακής πληροφορίας, διασφαλίζοντας, παράλληλα, τις αρχές της ανοιχτής κοινωνίας, τις συνταγματικές ελευθερίες και τα ατομικά δικαιώματα.

Αυτό επιτυγχάνεται με:

1. Εθνικό Σχέδιο Έκτακτης Ανάγκης στον Κυβερνοχώρο
2. Καθορισμός Βασικών Απαιτήσεων Ασφάλειας
3. Αντιμετώπιση Περιστατικών Ασφάλειας

Σύμφωνα με την Αρχή Προστασίας Προσωπικών Δεδομένων τα μέτρα ασφάλειας πρέπει να τεκμηριώνονται με κατάλληλα έγγραφα πολιτικής, όπως επιβάλλει η αρχή της λογοδοσίας. Παράλληλα, πρέπει να είναι αποδεδειγμένα επικυρωμένα από τη διοίκηση του υπευθύνου ή του εκτελούντος την επεξεργασία, ώστε να μην υπάρχει περιθώριο αμφισβήτησής τους.

Υπεύθυνοι και εκτελούντες επεξεργασία μπορούν να χρησιμοποιούν εγκεκριμένο κώδικα δεοντολογίας (σύμφωνα με το άρθρο 40 του ΓΚΠΔ) ή μηχανισμό πιστοποίησης (άρθρο 42 ΓΚΠΔ) για την απόδειξη της συμμόρφωσής τους, δηλαδή

προς απόδειξη ότι, καταρχήν, λαμβάνουν τα ενδεδειγμένα μέτρα ασφάλειας. Επισημαίνεται, βέβαια, ότι οι φορείς θα πρέπει να είναι σε θέση να αποδείξουν ότι τα εν λόγω μέτρα εφαρμόζονται αποτελεσματικά στην πράξη.

Συνεπώς, απαραίτητο βήμα για την απόδειξη της συμμόρφωσης είναι η καταγραφή των μέτρων ασφάλειας και η πιστοποίηση με πρότυπα και οδηγοί υλοποίησης πλαισίου ασφάλειας επεξεργασίας

Σήμερα, είναι διαθέσιμες διάφορες πιστοποιήσεις ασφάλειας πληροφοριακών συστημάτων, βασισμένες σε διεθνώς αποδεκτά πρότυπα, τα υφιστάμενα διεθνή πρότυπα είναι εξαιρετικά χρήσιμα, προκειμένου να βοηθήσουν έναν υπεύθυνο ή εκτελούντα στην επιλογή των κατάλληλων μέτρων μείωσης των κινδύνων μιας δραστηριότητας επεξεργασίας. Περαιτέρω, τα περισσότερα από τα πρότυπα είναι προσανατολισμένα στην ασφάλεια των πληροφοριακών συστημάτων και των δικτύων, συνεπώς απαιτείται κατάλληλη προσαρμογή, όπως για παράδειγμα για την ικανοποίηση των αρχών της ελαχιστοποίησης των δεδομένων και του χρονικού περιορισμού της επεξεργασίας.

**2. Αντικείμενο της υπηρεσίας**

**ΤΜΗΜΑ Α**

Στο πλαίσιο της αναβάθμισης, το έργο που θα υλοποιηθεί ως αναβάθμιση του υφιστάμενου συστήματος, έχει ως αντικείμενο την ενίσχυση της ηλεκτρονικής και δικτυακής ασφάλειας του Οργανισμού, στα πλαίσια των αναγκών και των αυξημένων απαιτήσεων της σύγχρονης εποχής και της ανακοινωθείσας εθνικής στρατηγικής για την κυβερνοασφάλεια 2020-2025.

Ειδικότερα, το Έργο αφορά στην αναβάθμιση και ολοκληρωμένη ανάπτυξη ενιαίου συστήματος κυβερνοασφάλειας με ετήσιες άδειες λειτουργείας που θα αναπτυχθεί στις υπάρχουσες υποδομές του Οργανισμού, προκειμένου να προσφέρει προστασία σε ολιστικό επίπεδο με αυτοματοποιημένους μηχανισμούς αναφοράς και αντιμετώπισης προκειμένου να διασφαλιστεί η επιχειρησιακή συνέχεια και η ακεραιότητα των συστημάτων και πληροφοριών του οργανισμού.

Τελικός στόχος είναι η θωράκιση της υπάρχουσας υποδομής των πληροφοριακών συστημάτων του οργανισμού καθώς και των υποστηριζόμενων ιστοσελίδων και υπηρεσιών που είναι διαθέσιμα στο κοινό, η εγκατάσταση και παραμετροποίηση δικτυακών και διαδικτυακών συστημάτων ελέγχου, καθώς και η προσθήκη νέων μέτρων ασφάλειας στο συνολικό δίκτυο των πληροφοριακών συστημάτων του οργανισμού.

Ακολούθως, βάσει των νέων μεθοδολογιών και αλγορίθμων ελέγχου της δικτυακής και διαδικτυακής επικοινωνίας των πληροφοριακών συστημάτων, θα προσδιοριστούν και θα θωρακισθούν έναντι κυβερνοεπιθέσεων όλα τα τρωτά σημεία στο σύνολο του δικτύου Η/Υ του οργανισμού που θα εντοπίσουν τα εγκατασταθησόμενα συστήματα. Τα ευρήματα και οι θωρακίσεις αυτών θα είναι συνεχώς διαθέσιμα σε αναλυτική αναφορά, όπου και θα αποτυπώνεται σε κάθε στιγμή και σε πραγματικό χρόνο, η τρέχουσα κατάσταση ασφάλειας του συνολικού δικτύου και υποδομών του οργανισμού και η διαδραστικότητα μεταξύ χρηστών, υποδομής και εν δυνάμει εισβολέων στην υποδομή.

Για την διασφάλιση της ασφαλούς επικοινωνίας των πληροφοριακών συστημάτων του Δήμου, καθώς και για την ασφαλή επεξεργασία των εγγράφων, αρχείων και πληροφοριών, η εγκατάσταση και παραμετροποίηση νέων συστημάτων ελέγχου και προστασίας του δικτύου Η/Υ του Δήμου κρίνεται απαράβατη.

Τα συστήματα ελέγχου που θα εγκατασταθούν από τον ανάδοχο, θα πρέπει να είναι ικανά να εκτελούν τις ακόλουθες διαδικασίες-διεργασίες:

- Με αυτοματοποιημένες διαδικασίες, να εντοπίζουν, να κατηγοριοποιούν και να απομονώνουν οποιαδήποτε ενέργεια ή προσπάθεια η οποία δεν συνάδει με την γνωστή συμπεριφορά των Η/Υ.
- Να αντιμετωπίζουν σε πραγματικό χρόνο, με βάση την παραμετροποίηση που έχει γίνει, τις απειλές που έχουν αναγνωριστεί, εκτελώντας τις κατάλληλες ενέργειες για την αντιμετώπισή τους.
- Να καταγράφουν όλα τα στοιχεία-δεδομένα (μη προσωπικού χαρακτήρα) του δικτύου Η/Υ με τα χαρακτηριστικά τους, όπως επίσης και τις αλλαγές που προκύπτουν στη ροή του χρόνου, παρέχοντας τη δυνατότητα αναγνώρισης "ξένων" οντοτήτων, απρόβλεπτων μεταβολών ή απωλειών.
- Να αναγνωρίζουν κακόβουλες ή επικίνδυνες ενέργειες, καθώς και να τις καταγράφουν για περαιτέρω διερεύνηση.
- Να αναγνωρίζουν σε κάθε σύστημα/υποσύστημα υπάρχοντα τρωτά σημεία που εντοπίζουν και αποτελούν είτε αιτία επίθεσης, είτε εν δυνάμει κίνδυνο, παρέχοντας παράλληλα και τον προτεινόμενο τρόπο αντιμετώπισης και διόρθωσης κάθε εκάστοτε περίπτωσης.
- Να παρακολουθούν και μελετούν την ευρύτερη συμπεριφορά χρηστών και υπολογιστών μέσα στο δίκτυο για την αναγνώριση περίεργων συμπεριφορών που δύνανται να συνιστούν περιπτώσεις εισβολής ή ρήγματος ασφαλείας.
- Να παρέχουν ασφάλεια με χρήση τεχνικών τεχνητής νοημοσύνης σε κάθε Device, Application και Network του οργανισμού.

- Να παρέχει πρόληψη απώλειας δεδομένων και να διασφαλίζει ότι οι κρίσιμες και ευαίσθητες πληροφορίες δεν αποστέλλονται εκτός του δικτύου του οργανισμού.

Για την εφαρμογή των εν λόγω μέτρων ασφαλείας που θα εφαρμοστούν από τον εγκατεστημένο εξοπλισμό και συστήματα, θα πρέπει να προσδιορισθούν όλα τα επίπεδα εκτέλεσης και εφαρμογής τους, καθώς και να διεξαχθούν ασκήσεις ετοιμότητας περιστατικών, για την διασφάλιση των πληροφοριακών συστημάτων, την τήρηση των μέτρων ασφαλείας κατά τη χρήση τους. Το προσωπικό του οργανισμού θα πρέπει να εκπαιδευθεί στα νέα συστήματα ελέγχου που θα εγκατασταθούν.

Οι στόχοι του προτεινόμενου έργου είναι:

1. Αναβαθμισμένη Θωράκιση του οργανισμού από κυβερνοεπιθέσεις - κυβερνοαπειλές.
2. Δημιουργία ενιαίου μηχανισμού αναφοράς περιστατικών.
3. Παραγωγή αναφορών σε πραγματικό χρόνο.
4. Εφαρμογή μέτρων πρόληψης και προστασίας.

**Τεχνικές Προδιαγραφές ΤΜΗΜΑΤΟΣ Α**

***Α.1 Αρχιτεκτονική Συστήματος***

Η προτεινόμενη αρχιτεκτονική πρέπει να εγγυάται την υψηλή ποιότητα και αποτελεσματική υποστήριξη για την συλλογή δεδομένων, την ανάλυση και επεξεργασία τους και την τελική αξιοποίηση τους από το σύστημα.

Η σχεδίαση της δικτυακής αρχιτεκτονικής του συστήματος θα γίνει με βάση τις λειτουργικές προδιαγραφές, οι οποίες θα προσδιοριστούν στην Μελέτη Εφαρμογής.

Για την ανάπτυξη της απαιτούμενης λειτουργικότητας, ο Ανάδοχος θα πρέπει να προτείνει: α) τη βέλτιστη προτεινόμενη αρχιτεκτονική,
β) τις προτεινόμενες διαδικασίες συλλογής δεδομένων και
γ) τρόπους αυτοματοποιημένων αποκρίσεων σε περιστατικά.

Οι χρήστες θα πρέπει να μπορούν να επικοινωνούν με το Πληροφορικό Σύστημα πλοηγούμενοι μέσα από διαδεδομένους WEB Browser (Internet Explorer, Mozilla, Chrome κτλ.). Ο χρήστης θα έχει τη δυνατότητα καταχώρισης ερωτημάτων αναζήτησης, στα οποία το σύστημα θα ανταποκρίνεται αντλώντας τη σχετική πληροφορία από τις αντίστοιχες βάσεις δεδομένων και παρουσιάζοντας τη στο

λεγόμενο επίπεδο παρουσίασης (presentationlayer). Η ανακτώμενη πληροφορία θα διατίθεται και σε εκτυπώσιμη μορφή.

Συνοπτικά ο υποψήφιος ανάδοχος πρέπει να παρέχει μια ολοκληρωμένη λύση Πληροφοριακού Συστήματος, η οποία θα αποτελείται από:

- Τον εξοπλισμό, το λογισμικό λειτουργικών συστημάτων και τα λογισμικά ανάπτυξης του Πληροφοριακού Συστήματος
- Τη μελέτη και το σχεδιασμό του λογικού μοντέλου δεδομένων του Πληροφοριακού Συστήματος
- Την εκπαίδευση χρηστών
- Την υποστήριξη λειτουργίας του Πληροφοριακού Συστήματος (helpdesk για όλα τα επίπεδα των χρηστών)
- Την εγγύηση καλής λειτουργίας
- Την εγγύηση συντήρησης

### Α.1.1 Απαιτήσεις Αρχιτεκτονικής Συστήματος

Το Σύστημα πρέπει να είναι «ανοικτής» αρχιτεκτονικής (open architecture) και θα χρησιμοποιεί πρότυπα που θα διασφαλίζουν:

- Την ομαλή συνεργασία και λειτουργία μεταξύ των επιμέρους λειτουργικών εφαρμογών της ολοκληρωμένης λύσης.
- Τη δικτυακή συνεργασία μεταξύ εφαρμογών ή / και συστημάτων, τα οποία βρίσκονται σε διαφορετικά υπολογιστικά συστήματα (π.χ. firewalls, servers κτλ).
- Η αρχιτεκτονική του συστήματος θα πρέπει να υποστηρίζει την πλήρη διασυνδεσιμότητα με τρίτα συστήματα ανεξάρτητα των τεχνολογιών ανάπτυξής τους.

Η ανοιχτή αρχιτεκτονική θα ακολουθηθεί, τόσο σε επίπεδο εξοπλισμού (εύκολη διασύνδεση, επέκταση, αντικατάσταση μερών, κ.λ.π.), όσο και σε επίπεδο λογισμικού εφαρμογών.

### Α.1.2 Τεχνολογίες και σχέδιο υλοποίησης Έργου

**Ο υποψήφιος Ανάδοχος θα πρέπει να προτείνει μια ολοκληρωμένη λύση. Η προτεινόμενη πλατφόρμα θα πρέπει να αποτελεί μια ολοκληρωμένη λύση open XDR (Extended Detection & Response) με χαρακτηριστικά και λειτουργίες Next Gen SOC, η οποία να εξασφαλίζει την κεντρική παρακολούθηση και διαχείριση, αποφεύγοντας άλλης παλαιού τύπου τεχνικές με την εγκατάσταση διαφορετικών ξεχωριστών απλών εργαλείων SIEM (Security Information & Events Management) και άλλων που εγκαθίσταται και διαχειρίζονται ξεχωριστά ή απαιτείται χειροκίνητη ξεχωριστή διαδικασία ενσωμάτωσής του.**

**Η πλατφόρμα πρέπει να έχει τη δυνατότητα συλλογής και επεξεργασίας από πολλαπλών τύπων πηγές δεδομένων και όχι μόνο αρχείων καταγραφής, κινούμενη στη φιλοσοφία του big data security analytics. Συνδυάζοντας πληροφορίες από δικτυακή κίνηση (network traffic), user data, cloud data, file data στόχος είναι η εξάλειψη πιθανών τυφλών σημείων και ο συσχετισμός όλων των δεδομένων για την παραγωγή καλύτερων αποτελεσμάτων. Μέσα από αυτοματοποιημένες διαδικασίες εμπλουτισμού και συσχετισμών, τα δεδομένα θα βελτιστοποιούνται για αξιοποίηση από μηχανισμούς έρευνας και εντοπισμού. Ειδικότερα με την εκμετάλλευση αυτοματοποιημένης επεξεργασίας και μηχανικής μάθησης, το σύστημα θα πρέπει να μπορεί να λειτουργεί αποτελεσματικά ως ένα ολοκληρωμένο κέντρο αναφοράς και αυτόματης πρότασης και λήψης αντιμέτρων. Το σύστημα θα πρέπει κατ' ελάχιστον να συνοδεύεται από τεχνολογίες SIEM, Sandbox, NTA, Threat Intelligence και IDS και να μην απαιτείται η ξεχωριστή προμήθεια λογισμικού.**

**Το προσφερόμενο σύστημα θα πρέπει να έχει τη δυνατότητα να υποστηρίζει και το μοντέλο MDR (Managed Detection & Response) και στο σύνολό του θα πρέπει να υποστηρίζει όλο τον κύκλο ζωής αναγνώρισης και αντιμετώπισης απειλών, που αναλύεται στα στάδια:**

- **Συλλογή (Collect)**
- **Εντοπισμός (Detect)**
- **Έρευνα (Investigate)**
- **Απόκριση (Respond)**

**Το υπό αναβάθμιση σύστημα θα πρέπει να περιλαμβάνει την προμήθεια, εγκατάσταση και παραμετροποίηση αισθητήρων ασφαλείας (φυσικών ή εικονικών), οι οποίοι θα εφαρμόζουν λειτουργίες ML-IDS, antivirus, sandboxing και NTA.**

### A.1.3 Χαρακτηριστικά Next Gen Soc

1. **Μοντέρνο περιβάλλον χρήσης (GUI) που ενσωματώνει άλλης άλλης απαραίτητες λειτουργίες παρακολούθησης και διαχείρισης.**
2. **Πρόσβαση με χρήση ρόλων χρηστών (RBAC – Role Based Access ) για την διαχείριση δικαιωμάτων (user privilege management)**
3. **Υποστήριξη πολλαπλών ενοίκων (multi-tenant) για την ξεχωριστή διαχείριση οντοτήτων, φυσικών δικτύων κτλ**
4. **Εφαρμογή ξεχωριστού μοντέλου μηχανικής μάθησης ανά tenant για τη βελτίωση άλλης ακρίβειας των αποτελεσμάτων και τη μείωση των εσφαλμένων θετικών συμβάντων (false positives), εφαρμόζοντας ξεχωριστά συμπεριφορικά μοντέλα.**

5. **Εξελιγμένες δυνατότητες μηχανικής μάθησης που να συμπεριλαμβάνουν τόσο supervised όσο και unsupervised διαδικασίες, τεχνολογίες graph ML και να συνδυάζονται μεταξύ άλλης για την παραγωγή βέλτιστων αποτελεσμάτων**
6. **Δυνατότητες ενσωμάτωσης με εργαλεία και τεχνολογίες ασφαλείας άλλης Firewalls, WAF, SWG, EDR, SOAR κτλ**
7. **Υποστήριξη API για ενσωμάτωση με άλλης τεχνολογίες άλλης HoneyPots, εργαλεία OSINT κτλ.**
8. **Μία ενοποιημένη, υψηλής απόδοσης, αποθήκη δεδομένων ("Big Data" High Speed Lake)**
9. **Δυνατότητα εγκατάστασης τόσο σε φυσικό εξοπλισμό, όσο και σε εικονικό ή περιβάλλον cloud**
10. **Κατανεμημένη και επεκτάσιμη αρχιτεκτονική που να υποστηρίζει ωστόσο και "All In One" σενάρια.**
11. **Υψηλή διαθεσιμότητας με τη χρήση clusters και ευέλικτη τήρηση και αποθήκευση δεδομένων.**
12. **Μηχανισμοί Συλλογής που να μπορούν να εγκατασταθούν τόσο σε φυσικό όσο και σε εικονικό περιβάλλον**
13. **Το σύστημα θα πρέπει να ακολουθεί ανοιχτή αρχιτεκτονική που να επιτρέπει την εισαγωγή δεδομένων από οποιαδήποτε συσκευή με τη χρήση Integration APIS.**
14. **Κεντροποιημένη διαχείριση**
15. **Απλό ενοποιημένο μοντέλο αδειών χωρίς επιπλέον κόστη**

### A.1.4 Next-Generation SIEM

**Η εφαρμογή θα πρέπει να βασίζεται σε μια ενοποιημένη αποθήκη δεδομένων βασισμένη στην αρχιτεκτονική του big data lake. Τα δεδομένα θα πρέπει κατ' ελάχιστον να μπορούν να εισαχθούν μέσω syslog. Όπου είναι εφικτό θα πρέπει να παρέχεται η χρήση parsers για άλλης κυριότερες και δημοφιλέστερες λύσεις δικτύων και ασφαλείας ώστε οι πληροφορίες να κανονικοποιούνται και να συσχετίζονται με αυτοματοποιημένο τρόπο.**

**Επιπλέον, θα πρέπει να παρέχονται οι παρακάτω ελάχιστες λειτουργικότητες:**

1. **Απλός όσο και εξεζητημένος μηχανισμός αναζήτησης που να βασίζεται σε λογικούς τελεστές (Boolean modifiers)**
2. **Οι αναζητήσεις να μπορούν να εφαρμοστούν ως μόνιμα φίλτρα σε όλο το περιβάλλον για ταχύτερη διερεύνηση και ανάλυση περιστατικών.**

3. **Υψηλής απόδοσης και άμεσες ανταποκρίσεις στην αναζήτηση και το φιλτράρισμα στο big data**
4. **Πρόσβαση σε πηγές δεδομένων και όχι μόνο σε syslog δεδομένα**
5. **Συλλογή δεδομένων από δικτυακή κίνηση ( μέσω TAP ή Mirror Traffic). Τα πακέτα θα πρέπει να γίνονται reduce, να κανονικοποιούνται και να μετατρέπονται σε αξιοποιήσιμα μετα-δεδομένα για την ενσωμάτωση στο big data lake.**
6. **Συλλογή δεδομένων από user sources όπως το Microsoft AD μέσω API Connector**
7. **Συλλογή δεδομένων από πηγές νέφους (cloud ) άλλης Office365 μέσω Connectors**
8. **Τα δεδομένα από τις πηγές πρέπει να κανονικοποιούνται, να εμπλουτίζονται και να συσχετίζονται αυτόματα από το σύστημα**
9. **Στις πηγές εμπλουτισμού θα πρέπει να περιλαμβάνονται γεωγραφικού προσδιορισμού (Geo-Awareness), IP Reputation, Threat Intelligence και DPI Application awareness.**
10. **Μοντέρνο περιβάλλον χρήστη με λειτουργίες SIEM που θα περιλαμβάνουν ερωτήματα και δημιουργίες κανόνων. Πρόσθετο για παραδοσιακή απεικόνιση SIEM (π.χ. Kibana)**

**Α.1.5 Εντοπισμός KillChain (KillChain Detections)**

**(συμπεριλαμβάνοντας IDS/Exploit, Malware και APT Sandboxing, Anti-Phishing κτλ.)**

1. **Το Σύστημα θα πρέπει να έχει ενσωματωμένους μηχανισμούς εντοπισμών σε κάθε φάση του CyberSecurity KillChain, συμπεριλαμβάνοντας Reconnaissance, Delivery, Exploitation, Installation, Command & Control, and Actions & Exfiltrations**
2. **Το Σύστημα θα πρέπει να περιλαμβάνει ενσωματωμένη βάση υπογραφών IDS, ενισχυμένη από ανάλυση μηχανικής μάθησης (ML-IDS)**
3. **Θα πρέπει να υποστηρίζει πολλαπλά Threat Intelligence Feeds, συμπεριλαμβάνοντας εμπορικές πηγές, open-source, anti-phishing κ.α.**
4. **Θα πρέπει να επιτρέπει ενσωμάτωση με 3rd party feeds μέσω STIX/TAXII και/ η MISP**
5. **Θα πρέπει να έχει ενσωματωμένες δυνατότητες APT Sandboxing για να αναγνωρίζει και να περιορίζει άγνωστα αρχεία, άλλης άλλης και για εντοπισμό ransomware, spyware.**

### Α.1.6 Ανάλυση Δικτύου (Network Traffic Analysis)

**Με την επιθεώρηση της δικτυακής κίνησης σε πραγματικό χρόνο, το σύστημα θα πρέπει να μπορεί να μοντελοποιήσει την κίνηση για αναγνώριση παράτυπων συμπεριφορών και ειδοποιήσεων.**

1. **Θα πρέπει να ενσωματώνει λειτουργικότητα Deep Packet Inspection (DPI) για την αναγνώριση τουλάχιστον 4000 εφαρμογών και να δομεί σχετικά συμπεριφορικά μοντέλα.**
2. **Τα δεδομένα κίνησης δικτύου θα πρέπει να μετασχηματίζονται σε κατάλληλα μετα-δεδομένα που περιλαμβάνουν και το payload, για την αντίστοιχη προαιρετική μείωση άλλης ανάγκης αποθηκευτικών χώρων.**
3. **Θα πρέπει να ενσωματώνει λειτουργικότητα NTA Detections, συμπεριλαμβάνοντας Application Usage Anomalies, Long App Session Anomalies, και Unapproved Asset Activity**
4. **Θα πρέπει να εντοπίζει ανωμαλίες στη συμπεριφορά των Firewalls, όπως άρνησης υπηρεσιών( denial anomalies) ή σε σχέση με κανόνες ορθής χρήσης rule usage anomalies**

### Α.1.7 User Behavior Analytics (UBA)

**Σε συνδυασμό με την ανάλυση πακέτων, το σύστημα θα πρέπει να μπορεί να συνδεθεί με πηγές δεδομένων χρηστών, όπως το MS Active Directory**

1. **Θα πρέπει να πραγματοποιεί ανάλυση και εντοπισμό ανωμαλιών στη συμπεριφορά του χρήστη (user behavior)**
2. **Θα πρέπει να ενσωματώνει μοντέλα εντοπισμού ανωμαλιών σε τοποθεσίες δικτύου που δεν έχουν οριστεί (Impossible Travel Anomaly) ή ώράριο που έγινε η αυθεντικοποίηση (Log In Time Anomaly)**
3. **Συνδυασμός με πληροφορίες που συλλέγονται από Network Trafic Analysis συστήματα, έτσι ώστε όλες οι ανιχνεύσεις (detections) και τα σχετικά Συμβάντα (events) στα αρχεία καταγραφής (logs) αλλά και τυχόν άλλες πηγές να συσχετίζονται αυτόματα.**

### Α.1.8 Endpoint Behavior Analytics (EBA)

**Εκτός από τα αναλυτικά δεδομένα δικτύου και χρηστών που περιγράφηκαν παραπάνω, το σύστημα θα πρέπει να μπορεί να συλλέγει δεδομένα από τελικές συσκευές (assets/endpoints) όπως Η/Υ, Εκτυπωτές, κ.α. οι οποίες υπάρχουν στο δίκτυο, να κάνει ανάλυση (analytics) και να εντοπίζει συμπεριφορικές ανωμαλίες.**

1. **Θα πρέπει να μπορεί να εισάγει δεδομένα από τρίτα συστήματα εντοπισμού ευπαθειών (vulnerability scanners) όπως Nessus, Tenable, Rapid7 και να συσχετίζει τα ευρήματα με σχετικά γεγονότα ασφαλείας που προκύπτουν.**

2. **Θα πρέπει να μπορεί να ανακαλύψει όλες τις τελικές συσκευές (assets/endpoints) σε ένα δίκτυο και να τις κατηγοριοποιεί με βάση τη διεύθυνση MAC και IP.**

3. **Η λίστα των ανακαλυφθέντων/εντοπισθέντων τελικών συσκευών (assets) θα πρέπει να μπορεί να επαυξάνεται και να παραμετροποιείται με τη χρήση αρχείων csv που περιέχουν λίστες και περιγραφές.**

4. **Θα πρέπει να μπορεί να καταγράψει όλους τους συσχετισμούς μιας τελικής συσκευής (asset) και να δίνει στοιχεία όπως IP διευθύνσεις, ιστορικά στοιχεία τη χρήση εφαρμογών κτλ.**

**Α.1.9 Ορατότητα Δικτύου και Υπηρεσιών (Network & Service Visibility)**

**Θα πρέπει να περιλαμβάνει αξιόπιστα εργαλεία απεικόνισης δικτύων και υπηρεσιών, με δυνατότητες ανάλυσης (analytics), με στόχο να προσφέρει ορατότητα που έχουν σχέση με τις επιδόσεις του δικτύου (network performance), την χρήση των εφαρμογών (application usage) κ.α.**

**Α.1.10 Κυνήγι Απειλών και Διερεύνηση (Threat Hunting & Investigation)**

**Σε συνδυασμό με τις πηγές δεδομένων στην ενοποιημένη βάση δεδομένων (unifed data lake), τα κανονικοποιημένα και συσχετισμένα δεδομένα θα πρέπει να είναι διαθέσιμα για περαιτέρω διερεύνηση και ανάυση τυχόν απειλών (threat hunting) οποιαδήποτε στιγμή.**

1. **Το σύστημα θα πρέπει να έχει ενσωματωμένα σχετικά εργαλεία, προκαθορισμένες αναζητήσεις και ερωτήματα, καθώς και οπτικοποιήσεις (visualizations) συμβάντων.**

2. **Οι οπτικοποιήσεις θα πρέπει να είναι παραμετροποιήσιμες ανάλογα με τις ανάγκες του πελάτη.**

3. **Το σύστημα θα πρέπει να προσφέρει δυνατότητες συσχετισμού από ερωτήματα που έχει κάνει ένας αναλυτής με τυποποιημένου τύπου κριτήρια , προκειμένου οι αναλυτές να δομήσουν πληροφορίες για διάφορους τύπους επιθέσεων (attack sequences) ή να απομονώσουν πληροφορίες χρήσιμες για αυτούς.**

4. **Όλα τα ερωτήματα θα πρέπει να μπορούν να αποθηκευτούν, επεξεργαστούν και αντιγραφούν από τους χρήστες.**

5. **Οι οπτικοποιήσεις θα πρέπει να μπορούν να αποθηκευτούν σαν οθόνες εργασίας (custom dashboards).**

6. **Τα ερωτήματα θα πρέπει να μπορούν να συνδυαστούν με αυτόματες**

**ενέργειες/αποκρίσεις (PlayBooks).**

### A.1.11 Playbooks / Integrated Orchestration & Response (SOAR)

1. **Το σύστημα πρέπει να συμπεριλαμβάνει μια βιβλιοθήκη με έτοιμες ενσωματωμένες αυτόματες αποκρίσεις (playbooks).**
2. **Οι ενσωματωμένες ενέργειες/αποκρίσεις θα πρέπει να συμπεριλαμβάνουν**
    - **Alerts – Αποστολή e-mail/slack message κτλ**
    - **Actions – Άνοιγμα μιας υπόθεσης (case), εκτέλεση μια εντολής API, δημιουργία ενός security event κτλ**
    - **Responses – Μπλοκάρισμα μιας IP στο Firewall, απενεργοποίηση ενός χρήστη στο Active Directory, εκτέλεση δέσμης ενεργειών κτλ**
3. **Παράλληλα με τις αυτοματοποιημένες ενέργειες, όπως το μπλοκάρισμα μιας IP θα πρέπει ο χρήστης να μπορεί μέσω της Διεπαφής χρήστη (User Interface) της πλατφόρμας να μπορεί να υλοποιήσει διερεύνηση, αντιμετώπιση ή και ανάλυσης του συμβάντος.**
4. **Δυνατότητα ενσωμάτωσης σε ήδη έτοιμα εμπορικά εργαλεία SOAR (security orchestration, automation and response)**

**<u>Επιπλέον Δυνατότητες</u>**

**Ειδοποιήσεις (Alarming)**

1. **Το σύστημα θα πρέπει να προσφέρει έναν έξυπνο, μοντέρνο και παραμετροποιήσιμο μηχανισμό ειδοποιήσεων που να δύναται να οριστεί με βάση παραλήπτες και άλλα κριτήρια (score severity, killchain category, etc.)**
2. **Οι ειδοποιήσεις θα πρέπει να μπορούν να αποσταλούν με email ή τύπου slack μηνύματα. Τα μηνύματα που θα αποστέλλονται πρέπει να είναι παραμετροποιήσιμα από τον χρήστη και το περιεχόμενο τους ανάλογο με το συμβάν που έχει δημιουργηθεί.**

**Αναφορές (Reporting)**

1. **Το σύστημα πρέπει να περιέχει ένα σύγχρονο εξελιγμένο μηχανισμό αναφορών που θα επιτρέπει παράλληλα εύκολη δημιουργία νέων αναφορών με drag and drop και αποθήκευσή για χρήση σε οποιοδήποτε σημείο.**
2. **Οι αναφορές θα πρέπει να παράγονται με χρονοπρογραμματισμό και να αποστέλλονται σε διαφορετικούς χρήστες.**
3. **Οι αναφορές θα πρέπει να αποστέλλονται με email σαν pdf ή csv ή να γράφονται σε αρχείο.**

4. **Το σύστημα θα πρέπει να περιλαμβάνει πληθώρα έτοιμων αναφορών (templates).**

**Portal (θα πρέπει να διαθέτει/προσφέρει)**

1. **Πρόσβαση των χρηστών βάση ρόλου (User RBAC access) στο Portal με συνολική ή περιορισμένη πρόσβαση σε πληροφορίες.**
2. **Προσαρμοσμένοι πίνακες ελέγχου (Custom Dashboards) ανά ρόλο χρήστη.**
3. **Χρονοπρογραμματισμένες αναφορές για κάθε tenant, tenant group και RBAC users.**

Η πρόσβαση των χρηστών θα πρέπει να μπορεί να περιορίζεται σε Read-Only, limited view, μέχρι full visibility and access

**ΤΜΗΜΑ Β**

Το **ISO 27001** (IT Information Management System) είναι ένα διεθνές πρότυπο για τη διαχείριση της ασφάλειας των πληροφοριών.
Στο πρότυπο αυτό περιγράφονται οι απαιτήσεις που πρέπει να πληροί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του. Έχει προετοιμαστεί για να παρέχει απαιτήσεις για τη δημιουργία, την εφαρμογή, τη συντήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών. Η υιοθέτηση του είναι μια στρατηγική απόφαση για έναν οργανισμό. Η δημιουργία και η εφαρμογή του επηρεάζεται από τις ανάγκες και τους στόχους του οργανισμού, τις απαιτήσεις ασφάλειας, τις οργανωτικές διαδικασίες που χρησιμοποιούνται και το μέγεθος και τη δομή του δήμου. Διατηρεί την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών εφαρμόζοντας μια διαδικασία διαχείρισης κινδύνων και δίνει εμπιστοσύνη στα ενδιαφερόμενα μέρη ότι η διαχείριση των κινδύνων γίνεται επαρκώς.
Το GDPR ενθαρρύνει τη χρήση συστημάτων πιστοποίησης όπως το ISO 27001, δεδομένου ότι στο πρότυπο αυτό περιγράφονται οι απαιτήσεις που πρέπει να πληροί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του και είναι σε θέση να επιδείξει ότι διαχειρίζεται ενεργά την ασφάλεια των δεδομένων του σύμφωνα με τις διεθνείς βέλτιστες πρακτικές.
Ο Δήμος μέσω της επιτήρησης και ανανέωσης της πιστοποίησης του τμήματος πληροφορικής θα συνεχίσει να λαμβάνει πολλαπλά οφέλη, μεταξύ των οποίων είναι:

- Προσδίδει εικόνα αξιοπιστίας και εμπιστοσύνης για τον Δήμο.
- Τεκμηριώνεται δέσμευση ως προς την ασφάλεια πληροφοριών από όλους και σε όλα τα επίπεδα του Δήμου.

- Διασφαλίζει την επαλήθευση τήρησης σχετικών νόμων και κανονισμών.
- Αποδεικνύει την γνώση του Δήμου σχετικά με την επάρκεια και συμμόρφωση του συστήματος ως προς την ασφαλή διαχείριση πληροφοριών.
- Βοηθά τον Δήμο να αναγνωρίσει, αξιολογήσει και διαχειριστεί κινδύνους ασφάλειας πληροφοριών.
- Δεδομένου ότι η εφαρμογή του GDPR δεν πιστοποιείται, η επίτευξη διαπιστευμένης πιστοποίησης σύμφωνα με το πρότυπο ISO 27001 παρέχει μια ανεξάρτητη και εξειδικευμένη αξιολόγηση για το αν ο Δήμος έχει εφαρμόσει τα κατάλληλα μέτρα για την προστασία των δεδομένων σας σύμφωνα με το GDPR.
- Ενίσχυση των τεχνολογικών μεθόδων και μέτρων ασφαλείας για τη διαχείριση των πληροφοριών.
- Υιοθέτηση πολιτικής για την αντιμετώπιση διαρροής πληροφοριών.
- Δημιουργία δικλείδων ασφαλείας για τον κίνδυνο διαρροής/απώλειας/κλοπής των δεδομένων.

Το διεθνές πρότυπο **ISO 27701** αποτελεί επέκταση των προτύπων ISO 27001 και ISO 27002 και σχεδιάστηκε, προκειμένου να ενισχύσει το υφιστάμενο σύστημα διαχείρισης ασφάλειας πληροφοριών με πρόσθετες απαιτήσεις, ώστε να αναπτυχθεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών και Προστασίας Προσωπικών Δεδομένων.
Το ISO 27701 ορίζει τις απαιτήσεις διαχείρισης των προσωπικών δεδομένων και παρέχει κατευθυντήριες οδηγίες για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εφαρμόζεται σε όλους τους οργανισμούς που επιθυμούν να διασφαλίσουν, παράλληλα με την ασφάλεια πληροφοριών, την προστασία των προσωπικών δεδομένων.
Προκειμένου ένας οργανισμός να πιστοποιηθεί κατά ISO 27701, πρέπει να διαθέτει ήδη πιστοποίηση ISO 27001 ή να επιλέξει την παράλληλη πιστοποίησή της με βάση τα δύο πρότυπα.
Η επιτήρηση/ανανέωση της πιστοποίησης κατά τα ανωτέρω διεθνή πρότυπα, αποδεικνύει τη δέσμευση του Δήμου:

- στην εφαρμογή πολιτικών που εξασφαλίζουν την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των πληροφοριών
- στην πλήρη συμμόρφωσή σας με τις ισχύουσες νομοθετικές απαιτήσεις διαχείρισης προσωπικών δεδομένων (GDPR – General Data Protection Regulation).

**Τεχνικές Προδιαγραφές ΤΜΗΜΑΤΟΣ Β**

**<u>Για την ανανέωση του συστήματος ISO 27001 και ISO 27701 θα απαιτηθούν από τον Ανάδοχο τα παρακάτω βήματα και για τα δύο πρότυπα:</u>**

- Καταγραφή και αξιολόγηση υφιστάμενης κατάστασης.
- Διενέργεια Αξιολόγησης Επικινδυνότητας.
- Εσωτερικός Έλεγχος κατά ISO
- Έλεγχος του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με την Έκθεση αναφορά της επιθεώρησης
- Ενημέρωση–Εκπαίδευση -Εφαρμογή.
- Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO27001.

## 3. Χρονοδιάγραμμα και Φάσεις Υπηρεσίας για ΤΜΗΜΑΤΑ Α και Β

### 3.1 Χρονοδιάγραμμα και Φάσεις Υπηρεσίας για ΤΜΗΜΑΤΑ Α και Β

*Πίνακας 1: Χρονοδιάγραμμα υλοποίησης της υπηρεσίας*

| Α/Α Φάσης | Τίτλος Φάσης | Μήνας Έναρξης | Μήνας Λήξης (παράδοσης) |
|---|---|---|---|
| 1 | Μελέτη Υλοποίησης | **1** | **1** |
| 2 | Προμήθεια, εγκατάσταση και παραμετροποίηση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας | **1** | **1** |
| 3 | Εκπαίδευση | **1** | **1** |
| 4 | Πιλοτική λειτουργία | **1** | **1** |
| 5 | Παραγωγική λειτουργία | **1** | **2** |
| 6 | Άδειες Χρήσης | **1** | **24** |
| 7 | Εγγύηση καλής λειτουργίας (Δωρεάν Συντήρηση) | **2** | **24** |
| 8 | Προετοιμασία ανανέωσης ISO 27001, ISO 27701 | **2,14** | **5,17** |
| 9 | Επιθεώρηση και Ανανέωση ISO 27001, ISO 27701 | **5,17** | **8,20** |

### 3.2 Φάσεις Υλοποίησης της Υπηρεσίας

**ΦΑΣΗ Νο 1: Μελέτη Υλοποίησης**
Στόχοι:
Η μελέτη υλοποίησης αφορά στην αποτύπωση και οριστικοποίηση των προδιαγραφών υλοποίησης του συστήματος κυβερνοασφάλειας.

Περιγραφή Υλοποίησης:
Η μελέτη θα περιλαμβάνει κατ' ελάχιστον τις παρακάτω απαιτήσεις / ενέργειες:
Σχέδιο Διαχείρισης και Ποιότητας Έργου (ΣΔΠΕ)
Τον πλήρη και λεπτομερή σχεδιασμό του συνολικού συστήματος
Παραδοτέα:
Π.1: Μελέτη Υλοποίησης

**ΦΑΣΗ Νο 2: Προμήθεια, εγκατάσταση και παραμετροποίηση εξοπλισμού και λογισμικού συστήματος και Άδειες Χρήσης συστήματος**

Στόχοι:
Προμήθεια νέου εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας βάσει της αναβάθμισης του συστήματος.
Εγκατάσταση εξοπλισμού και λογισμικού συστήματος κυβερνοασφάλειας.
Παραμετροποίηση πληροφοριακών συστημάτων και λογισμικού συστήματος
Διενέργεια δοκιμών κυβερνοασφάλειας.
Άδειες Χρήσης συστήματος
Περιγραφή Υλοποίησης:
Περιλαμβάνει το σύνολο του απαιτούμενου εξοπλισμού για την υλοποίηση του έργου την εγκατάσταση του και παραμετροποίηση του.
Εγκατάστασή λογισμικού συστήματος και θέση του σε λειτουργία.
Παραδοτέα:
Π.2: Προμήθεια εξοπλισμού και λογισμικού συστήματος – Άδειες Συστήματος

**ΦΑΣΗ Νο 3: Εκπαίδευση**

Στόχοι: Εκπαίδευση χρηστών / διαχειριστών του συστήματος βάσει της αναβάθμισης του συστήματος.
Περιγραφή Υλοποίησης:
Οι δράσεις εκπαίδευσης, χρηστών / διαχειριστών του συστήματος περιλαμβάνουν:
την εκπαίδευση διαχειριστών του συστήματος
Παραδοτέα:
Π.3.1: Πρόγραμμα εκπαίδευσης
Π.3.2: Εκπαιδευτικό υλικό

**ΦΑΣΗ Νο 4: Πιλοτική Λειτουργία**

Στόχοι:
Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την εξασφάλιση της ομαλής μετάβασης του συστήματος έπειτα από την αναβάθμιση και την συντήρηση του στην κανονική λειτουργία του έργου με την υποστήριξη από τον ανάδοχο.
Εκπαίδευση (on the job training) χρηστών / διαχειριστών του συστήματος.
Στην φάση αυτή θα ελέγχει την ορθή λειτουργία του έργου, θα πραγματοποιηθούν οι απαραίτητες αλλαγές και προσαρμογές, και θα πραγματοποιηθούν οι δοκιμές ασφάλειας.

Περιγραφή Υλοποίησης:
1. Υποστήριξη λειτουργίας

Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλιση της πιλοτικής λειτουργίας όλου του πληροφοριακού συστήματος.
Περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:
Υποστήριξη λειτουργίας υλικού και λογισμικού συστήματος –εφαρμογών.
Αντιμετώπιση περιστατικών ασφαλείας.
On the Job training.
Παρακολούθηση κατάσταση ασφαλείας.
Τελική Παραμετροποίηση πληροφοριακού συστήματος

Παραδοτέα
Π.4. : Πιλοτική λειτουργία
Π.4.1: Υποστήριξη πιλοτικής λειτουργίας πληροφοριακού συστήματος
Π.4.2: On the Job training
Π.4.3: εκσφαλμάτωση πληροφοριακού συστήματος. Τελική Παραμετροποίηση πληροφοριακού συστήματος

**ΦΑΣΗ Νο 5: Παραγωγική Λειτουργία**
Στόχοι:
Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την εξασφάλισης της κανονικής λειτουργίας όλου του πληροφοριακού συστήματος έπειτα από την αναβάθμιση και την συντήρηση του με την υποστήριξη από τον ανάδοχο.
Έλεγχος της ορθής λειτουργία του συστήματος.

Περιγραφή Υλοποίησης:
<u>Τεκμηρίωση Συστήματος (Τ.Σ.).</u>
Περιλαμβάνει την πλήρη και αναλυτική τεκμηρίωση του συστήματος που απαιτείται για την υποστήριξη της λειτουργίας του υλικού και του λογισμικού συστήματος και εφαρμογών.
<u>Υποστήριξη λειτουργίας</u>
Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλισης της κανονικής λειτουργίας όλου του συστήματος.
Περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:
Υποστήριξη λειτουργίας υλικού και λογισμικού συστήματος – εφαρμογών.
Αντιμετώπιση περιστατικών ασφαλείας
On the Job training.
Παρακολούθηση κατάστασης ασφαλείας
Τελική Παραμετροποίηση πληροφοριακού συστήματος

Παραδοτέα:
Π.5. : Παραγωγική λειτουργία
Π.5.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης

**ΦΑΣΗ Νο 6: Αδειών Χρήσης - Μηνιαία αναφορά**
Στόχοι:
Περιλαμβάνει την απαραίτητη ανανέωση των ετήσιων αδειών του Συστήματος Κυβερνοασφάλειας από τον ανάδοχο καθώς και μηνιαίες αναφορές ασφαλείας με

περιστατικά και αναφορές από το σύστημα καθώς και προς βελτίωση εισηγήσεις για το σύνολο της ασφάλειας του οργανισμού.

Παραδοτέα:
Π.6.1: Ετήσιο αναφορά ανανέωσης αδειών χρήσης
Π6.2: Μηνιαία αναφορά περιστατικών ασφαλείας

**ΦΑΣΗ Νο 7: Εγγύηση Καλής Λειτουργίας**
Στόχοι:
Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την εξασφάλισης της κανονικής λειτουργίας όλου του έργου και την συντήρηση του με την υποστήριξη από τον ανάδοχο.

Περιγραφή Υλοποίησης:
Υποστήριξη λειτουργίας –Συντήρησης
Περιλαμβάνει όλες τις απαραίτητες ενέργειες και την εξασφάλισης της κανονικής λειτουργίας όλου του συστήματος.
Περιλαμβάνει κατ' ελάχιστον τα ακόλουθα:
Προληπτική και διορθωτική συντήρηση εξοπλισμού
Υποστήριξη λειτουργίας υλικού και λογισμικού
Τηλεφωνική υποστήριξη–Helpdesk
Εποπτεία / διαχείριση συστημάτων ασφαλείας
Αντιμετώπιση περιστατικών ασφαλείας

**ΦΑΣΗ Νο 8: Προετοιμασία ανανέωσης ISO 27001, ISO 27701**
Στόχοι:
Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την προετοιμασία της ανανέωσης πιστοποίησης κατά ISO 27001 και ISO 27701

Περιγραφή Υλοποίησης:

Καταγραφή και αξιολόγηση υφιστάμενης κατάστασης.
Διενέργεια Αξιολόγησης Επικινδυνότητας.
Εσωτερικός Έλεγχος κατά ISO 27001 kai ISO 27701
Έλεγχος του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών σύμφωνα με την
Έκθεση αναφορά της επιθεώρησης
Παραδοτέα:
Π.8.: Έκθεση αναφοράς δραστηριοτήτων ISO 27001 – ISO 27701

**ΦΑΣΗ Νο 9: Επιθεώρηση και Ανανέωση ISO 27001, ISO 27701**
Στόχοι:
Περιλαμβάνει όλες τις απαραίτητες ενέργειες για την Επιθεώρηση της ανανέωσης πιστοποίησης κατά ISO 27001 και ISO 27701

Περιγραφή Υλοποίησης:

Ενημέρωση–Εκπαίδευση -Εφαρμογή.

Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO27001 και ISO 27701.

Παραδοτέα:

Π.9.1.: Έκθεση αναφοράς Εκπαίδευσης

Π.9.2: Έκθεση αναφοράς Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO27001 και ISO 27701

### 3.3 Παραδοτέα έργου

- Π.1: Μελέτη Υλοποίησης
- Π.2: Προμήθεια εξοπλισμού και λογισμικού συστήματος
- Π.3.1: Πρόγραμμα εκπαίδευσης
- Π.3.2: Εκπαιδευτικό υλικό
- Π.4. : Πιλοτική λειτουργία
- Π.4.1: Υποστήριξη πιλοτικής λειτουργίας πληροφοριακού συστήματος
- Π.4.2: On the Job training
- Π.4.3: Εκσφαλμάτωση πληροφοριακού συστήματος. Τελική Παραμετροποίηση πληροφοριακού συστήματος
- Π.5: Παραγωγική λειτουργία
- Π.5.1: Έντυπο και ηλεκτρονικό υλικό τεκμηρίωσης
- Π.6.: Ετήσιο report ανανέωσης αδειών χρήσης
- Π.8.: Έκθεση αναφοράς δραστηριοτήτων ISO 27001 – ISO 27701
- Π.9.1.: Έκθεση αναφοράς Εκπαίδευσης
- Π.9.2: Έκθεση αναφοράς Πιστοποίηση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών ISO27001 και ISO 27701

Όλα τα παραδοτέα πρέπει να υποβάλλονται και σε ηλεκτρονική μορφή. Όλα τα παραδοτέα πρέπει να παραχθούν και να γίνουν αποδεκτά από την Αναθέτουσα Αρχή εντός του συμβατικού χρόνου υλοποίησης του έργου. Όλα τα ανωτέρω παραδοτέα είναι υποχρεωτικά.

## 4. Προδιαγραφές Υπηρεσίας

### 4.1 Κριτήριο Ανάθεσης

Η σύμβαση θα ανατεθεί με το κριτήριο της πλέον συμφέρουσας από οικονομική άποψη προσφοράς, βάσει βέλτιστης σχέσης ποιότητας – τιμής, και η βαθμολόγηση των τεχνικών προσφορών θα βασίζεται στα κάτωθι κριτήρια:

| Α/Α | Κριτήρια Αξιολόγησης | Συντελεστής βαρύτητας |
|---|---|---|
| 1. | Συνολική προσέγγιση Αναδόχου | 15% |
| 1.1 | Κατανόηση Περιβάλλοντος και Ειδικών Απαιτήσεων | 10% |
| 1.2 | Οριζόντιες Απαιτήσεις: Διαλειτουργικότητα, Ασφάλεια και προστασία ιδιωτικότητας | 5% |
| 2. | Τεχνικές & Λειτουργικές Δυνατότητες προσφερόμενης λύσης | 10% |
| 2.1 | Λειτουργικά και τεχνολογικά χαρακτηριστικά | 10% |
| 3. | Προσφερόμενες υπηρεσίες | 50% |
| 3.1 | Υπηρεσίες ανανέωσης, συντήρησης, αναβάθμισης συστήματος κυβερνοασφάλειας | 30% |
| 3.2 | Υπηρεσίες Επιτήρησης / Ανανέωσης πιστοποίησης κατά ISO 27001 – 27701 | 20% |
| 4. | Διοίκηση, Διαχείριση και Ομάδα Έργου | 25% |
| 4.1 | Οργάνωση Υλοποίησης Έργου (Μεθοδολογία, Χρονοδιάγραμμα, Παραδοτέα) | 15% |
| 4.2 | Ομάδα Έργου | 10% |
| | ΣΥΝΟΛΟ | 100% |

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

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

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

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

$$T= \sigma 1 \chi K1 + \sigma 2 \chi K2 + \ldots\ldots + \sigma \nu \chi K\nu$$

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

Πλέον συμφέρουσα από οικονομική άποψη προσφορά είναι εκείνη που παρουσιάζει τον μικρότερο λόγο της προσφερθείσας τιμής προς τη συνολική βαθμολογία της τεχνικής προσφοράς (ήτοι αυτή στην οποία το Λ είναι ο μικρότερος αριθμός), σύμφωνα με τον τύπο που ακολουθεί.

$$\Lambda = \frac{\textbf{Προσφερθείσα τιμή}}{\textbf{Συνολική βαθμολογία τεχνικής προσφοράς}}$$

### 4.2 Οικονομική και χρηματοοικονομική επάρκεια Αναδόχου

Οι οικονομικοί φορείς που θα συμμετέχουν στη διαδικασία σύναψης της σύμβασης απαιτείται να έχουν μέσο γενικό ετήσιο κύκλο εργασιών για τις τρεις (3) τελευταίες οικονομικές χρήσεις ή, τις οικονομικές χρήσεις κατά τις οποίες ο οικονομικός φορέας δραστηριοποιείται, αν είναι λιγότερες από τρεις (2019-2020-2021) συνολικά μεγαλύτερο από το 200% του προϋπολογισμού του υπό ανάθεση Έργου.

Για την απόδειξη της οικονομικής και χρηματοοικονομικής επάρκειας της ανωτέρω παραγράφου οι οικονομικοί φορείς προσκομίζουν:

«Ισολογισμούς ή αποσπάσματα ισολογισμών, των τριών (3) τελευταίων ετών στις περιπτώσεις όπου η δημοσίευσή τους είναι υποχρεωτική σύμφωνα με την περί εταιρειών νομοθεσία της χώρας όπου είναι εγκατεστημένος ο οικονομικός φορέας . Σε περίπτωση που σύμφωνα με την νομοθεσία ο οικονομικός φορέας δεν υποχρεούται σε δημοσίευση ισολογισμού, τότε θα πρέπει να υποβάλλει υπεύθυνη δήλωση για τον κύκλο εργασιών συνοδευόμενη από τα σχετικά επίσημα στοιχεία που υπάρχουν ( π.χ. δηλώσεις φορολογίας εισοδήματος, δηλώσεις Φ.Π.Α. κ.λ.π.). Ομοίως σε περίπτωση που δεν έχει ακόμη ολοκληρωθεί η δημοσίευση του ισολογισμού του τελευταίου οικονομικού έτους υποβάλλεται υπεύθυνη δήλωση συνοδευόμενη από τα σχετικά επίσημα στοιχεία που υπάρχουν ( π.χ. δηλώσεις φορολογίας εισοδήματος, δηλώσεις Φ.Π.Α. κ.λ.π.) για το έτος αυτό.

Επιχειρήσεις που λειτουργούν ή ασκούν επιχειρηματική δραστηριότητα για χρονικό διάστημα που δεν επιτρέπει την έκδοση κατά νόμο τριών ισολογισμών, υποβάλλουν τους ισολογισμούς που έχουν εκδοθεί και τα σχετικά επίσημα στοιχεία που υπάρχουν κατά το διάστημα αυτό ( π.χ. δηλώσεις φορολογίας εισοδήματος, δηλώσεις Φ.Π.Α. κ.λ.π.).

*Στην περίπτωση που ο υποψήφιος Ανάδοχος είναι ένωση προσώπων, πρέπει να υποβάλει τα ανωτέρω έγγραφα χωριστά για καθένα από τα μέλη της. Στην περίπτωση αυτή επιτρέπεται η μερική κάλυψη των προϋποθέσεων από τα μέλη της Ένωσης αρκεί αυτές να καλύπτονται συνολικά.»*

### 4.3 Τεχνική και Επαγγελματική Ικανότητα Αναδόχου

#### 4.3.1 Επαγγελματική ικανότητα

Οι οικονομικοί φορείς που θα συμμετέχουν στη διαδικασία σύναψης της σύμβασης απαιτείται:

Να διαθέτουν την κατάλληλα τεκμηριωμένη και αποδεδειγμένη επαγγελματική ικανότητα στην υλοποίηση έργων αντίστοιχου μεγέθους και πολυπλοκότητας με το υπό ανάθεση Έργο.

Να έχουν ολοκληρώσει επιτυχώς κατά τα τελευταία τέσσερα (4) έτη* (τρέχον έτος προκήρυξης του διαγωνισμού, συν τα δύο προηγούμενα - ως έτος θεωρείται το σύνολο των ημερών από 1/1 έως 31/12):

- Τουλάχιστον δύο (2) έργα με αντικείμενο την εγκατάσταση ή/και ανανέωση ή/και συντήρηση ή/και αναβάθμιση ή/και αδειών χρήσης ολοκληρωμένου συστήματος κυβερνοασφάλειας αθροιστικά αξίας εξήντα χιλιάδων ευρώ (60.000€)
- Τουλάχιστον ένα (1) έργο με αντικείμενο την επιτήρηση / ανανέωση πιστοποιήσεων κατά ISO 27001 και 27701 σε φορείς του δημοσίου, Ν.Π.Δ.Δ., Ο.Τ.Α (Οργανισμό Τοπικής Αυτοδιοίκησης)

Για την απόδειξη της επαγγελματικής ικανότητας της ανωτέρω παραγράφου οι οικονομικοί φορείς προσκομίζουν:

Κατάλογο των κυριότερων υπηρεσιών που παρασχέθηκαν ο οποίος θα περιλαμβάνει τα κάτωθι στοιχεία εμπειρίας σε πίνακα ως εξής:

| Α/Α | ΠΕΛΑΤΗΣ | ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ | ΔΙΑΡΚΕΙΑ ΕΚΤΕΛΕΣΗΣ ΕΡΓΟΥ | ΠΡΟΫΠΟ-ΛΟΓΙΣΜΟΣ | ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΣΥΝΕΙΣΦΟΡΑΣ ΣΤΟ ΕΡΓΟ (αντικείμενο) | ΠΟΣΟΣΤΟ ΣΥΜΜΕΤΟΧΗΣ ΣΤΟ ΕΡΓΟ (προϋπολογισμός) | ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ (τύπος & ημ/νία) |
|---|---|---|---|---|---|---|---|

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

όπου «**ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ**»:

- εάν μεν ο αποδέκτης είναι αναθέτουσα αρχή, από συμβάσεις και πιστοποιητικά ορθής εκτέλεσης αυτών που έχουν εκδοθεί ή θεωρηθεί από την αρμόδια αρχή, στα οποία περιγράφεται οι παρεχόμενη υπηρεσία και θα αναφέρεται ο χρόνος υλοποίησης της και θα βεβαιώνεται ότι αυτή εκτελέστηκε έντεχνα και εντός των εγκεκριμένων χρονοδιαγραμμάτων και
-εάν δε ο αποδέκτης είναι ιδιωτικός φορέας, με αντίστοιχη δήλωση του αποδέκτη.

Εφόσον δεν είναι δυνατή η προσκόμιση των παραπάνω, προσκομίζεται υπεύθυνη δήλωση του οικονομικού φορέα, στην οποία θα αναφέρεται ο λόγος για τον οποίο δεν κατέστη εφικτή η προσκόμιση των παραπάνω δικαιολογητικών και η οποία θα συνοδεύεται από αντίγραφο του τιμολογίου και, εφόσον υφίσταται, της σχετικής σύμβασης.

#### 4.3.2 Ομάδα Έργου

Η Ομάδα Έργου θα πρέπει να διαθέτει την κατάλληλη εμπειρογνωσία καθώς και την ικανότητα εκπλήρωσης των καθηκόντων της στον τομέα της Κυβερνοασφάλειας και να αποτελείται κατ'ελάχιστο από:

- Έναν (1) Υπεύθυνο Έργου, πτυχιούχο και μεταπτυχιακό ΠΕ Τμήματος Πληροφορικής, με εμπειρία τουλάχιστον πέντε (5) έτη στην υποστήριξη πληροφοριακών συστημάτων.
- Έναν (1) Μηχανικό Ασφάλειας στον Κυβερνοχώρο (Cyber Security Engineer) με πτυχίο τριτοβάθμιας εκπαίδευσης και τέσσερα χρόνια εμπειρίας στο χώρο της πληροφορικής
- Δύο (2) Αναλυτές ασφάλειας στον κυβερνοχώρο (Cyber Security Analyst)
- Έναν (1) Μηχανικό Δικτύου (Network Engineer) με τέσσερα έτη εργασιακής εμπειρίας
- Έναν (1) υπεύθυνο προστασίας προσωπικών δεδομένων (Data Protection Officer), με τουλάχιστον 2ετή επαγγελματική εμπειρία σε θέματα του Κανονισμού Προστασίας Προσωπικών Δεδομένων και πιστοποίηση Υπευθύνου Προστασίας Προσωπικών Δεδομένων.
- Έναν (1) Υπεύθυνο Διαχείρισης συστημάτων ISO 27001 - 27701 με πτυχίο τριτοβάθμιας εκπαίδευσης και τουλάχιστον 5 χρόνια εμπειρία στις συμβουλευτικές υπηρεσίες πιστοποίησης κατά ISO 27001 – 27701

Οι οικονομικοί φορείς απαιτείται να διαθέτουν ομάδα έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την ανάληψη του Έργου.

Για την απόδειξη του ανωτέρω κριτηρίου ποιοτικής επιλογής οι οικονομικοί φορείς υποβάλλουν τα ακόλουθα στοιχεία τεκμηρίωσης:

- Πίνακας των **υπαλλήλων του Οικονομικού Φορέα** που συμμετέχουν στην Ομάδα Έργου, σύμφωνα με το ακόλουθο υπόδειγμα:

| Α/Α | Εταιρεία (σε περίπτωση Ένωσης / Κοινοπραξίας) | Ονοματεπώνυμο Μέλους Ομάδας Έργου | Θέση στην Ομάδα Έργου | Ανθρωπομήνες | Ποσοστό συμμετοχής* (%) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| **ΜΕΡΙΚΟ ΣΥΝΟΛΟ (1)** | | | | | |

- Ο Οικονομικός Φορέας, συμπληρωματικά με τον παραπάνω Πίνακα, θα πρέπει να καταθέσει υπεύθυνες δηλώσεις συνεργασίας, των εξωτερικών συνεργατών και των υπεργολάβων. Οι εξωτερικοί Συνεργάτες και οι υπεργολάβοι, θα δηλώνουν ότι το έργο (αντικείμενο της παρούσας Διακήρυξης), καθώς και οι υποχρεώσεις που απορρέουν από αυτό, τελούν σε γνώση τους. Τέλος, βιογραφικά σημειώματα της Ομάδας Έργου.

### 4.4 Πρότυπα Διασφάλισης Ποιότητας του Αναδόχου

Οι οικονομικοί φορείς που θα συμμετέχουν στη διαδικασία σύναψης της σύμβασης απαιτείται να διαθέτουν Πρότυπα διασφάλισης ποιότητας ως κάτωθι:
α) το πρότυπο EN ISO 9001:2015 - Σύστημα διαχείρισης ποιότητας
β) το πρότυπο EN ISO 27001:2013 - Σύστημα διαχείρισης για την ασφάλεια των πληροφοριών
γ) το πρότυπο ISO/ IEK 27701:2019-Σύστημα διαχείρισης προσωπικών δεδομένων
δ) το πρότυπο ISO 22301:2019 Σύστημα διαχείρισης επιχειρησιακής συνέχειας
ε)το πρότυπο ISO 37001:2017 Σύστημα διαχείρισης για την καταπολέμηση της δωροδοκίας

Με πεδίο εφαρμογής την εγκατάστασης συστημάτων Κυβερνοασφάλειας.

Για την απόδειξη της συμμόρφωσής τους με πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης της παραγράφου 4.3, οι οικονομικοί φορείς προσκομίζουν πιστοποιητικά συστήματος διαχείρισης ποιότητας (ISO ή ισοδύναμο) εν ισχύ, από διαπιστευμένο φορέα, στο πεδίο που ζητείται ή άλλα αποδεικτικά στοιχεία για ισοδύναμα μέτρα διασφάλισης ποιότητας, εφόσον ο υποψήφιος 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.

### 4.5 Λοιπές υποχρεώσεις

- Προσφορές υποβάλλονται για όλα τα τμήματα που αναφέρονται στην μελέτη.
- Η Διάρκεια του έργου είναι 24 μήνες.
- Ο χρόνος ισχύος των προσφορών που θα κατατεθούν κατά την διενέργεια της διαδικασίας θα είναι 8 μήνες.
- Η πληρωμή του αναδόχου για την προμήθεια του συνόλου των υπηρεσιών, θα πραγματοποιηθεί ως εξής: Απολογιστικές πληρωμές βάσει των παραδοτέων και εργασιών που έχουν ολοκληρωθεί για το χρονικό διάστημα αναφοράς για κάθε φάση και με την προσκόμιση των νόμιμων παραστατικών και δικαιολογητικών που προβλέπονται από τις διατάξεις του άρθρου 200 παρ. 5 του ν. 4412/2016[1] όπως τροποποιήθηκε και ισχύει, καθώς και κάθε άλλου δικαιολογητικού που τυχόν ήθελε ζητηθεί από τις αρμόδιες υπηρεσίες που διενεργούν τον έλεγχο και την πληρωμή.

**5. Προϋπολογισμός υπηρεσίας**

Ο προϋπολογισμός για το έργου παρουσιάζεται στον παρακάτω πίνακα:

| **Α/Α** | **ΥΠΗΡΕΣΙΕΣ** | **ΜΟΝΑΔΑ ΜΕΤΡΗΣΗΣ** | **ΠΟΣΟΤΗΤΑ** | **ΤΙΜΗ ΜΟΝΑΔΑΣ (€)** | **ΠΟΣΟ ΠΡΟ ΦΠΑ (€)** |
|---|---|---|---|---|---|
| 1 | ΑΝΑΝΕΩΣΗ, ΣΥΝΤΗΡΗΣΗ ΚΑΙ ΑΝΑΒΑΘΜΙΣΗ ΣΥΣΤΗΜΑΤΟΣ ΚΥΒΕΝΟΑΣΦΑΛΕΙΑΣ ΔΗΜΟΥ ΧΕΡΣΟΝΗΣΟΥ ΠΟΥ ΑΦΟΡΑ ΣΕ 150 IP's | ΚΑΤ' ΑΠΟΚΟΠΗΝ/ΕΤΟΣ | 2 | 30.000,00 | 60.000,00 |
| 2 | Υπηρεσίες Επιτήρησης/Ανανέωσης Πιστοποίησης ISO 27001 για δύο (2) χρόνια | ΑΝΘΡΩΠΟΜΗΝΕΣ | 8 | 2.500,00 | 20.000,00 |
| 3 | Υπηρεσίες Επιτήρησης/Ανανέωσης Πιστοποιήσης ISO 27701 για δύο (2) χρόνια | ΑΝΘΡΩΠΟΜΗΝΕΣ | 8 | 2.500,00 | 20.000,00 |
| | | | | **ΣΥΝΟΛΟ ΠΡΟ ΦΠΑ** | **100.000,00 €** |
| | | | | **ΦΠΑ 24%** | **24.000,00 €** |
| | | | | **ΣΥΝΟΛΙΚΟ ΠΟΣΟ** | **124.000,00 €** |

[1] Άρθρο 200 παρ. 5 ν. 4412/2016, όπως τροποποιήθηκε με το άρθρο 102 του ν. 4782/2021.

Η δαπάνη για την εν λόγω σύμβαση βαρύνει τον Κ.Α.: 10.6112.0001 και τίτλο « ΥΠΗΡΕΣΙΕΣ ΕΦΑΡΜΟΓΗΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΚΑΙ ΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ (CYBER SECURITY) ΣΤΟ ΔΙΚΤΥΟ Η/Υ ΤΟΥ ΔΗΜΟΥ ΧΕΡΣΟΝΗΣΟΥ» και ποσό 37.200,00 ανά έτος και τον Κ.Α.: 00.6117.0003 και τίτλο Υπηρεσίες πιστοποίησης κατά ISO 27001, ISO 27701, ISO 45001» και ποσό 24.800,00 ανά έτος.

**6.Πίνακες Συμμόρφωσης του Αναδόχου**

**ΟΜΑΔΑ Α**

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα θα πρέπει να είναι ανοιχτού τύπου επιτρέποντας την διασύνδεση συστημάτων ασφαλείας ανεξαρτήτου προμηθευτή (Open XDR). | ΝΑΙ. Να περιγραφεί ο προτεινόμενος μηχανισμός | | |
| | Το σύστημα θα πρέπει να υποστηρίζει λειτουργία SIEM και θα μπορεί να αναπτυχθεί σε όλα τα περιβάλλοντα για να παρέχει διάχυτη ορατότητα. Η τεχνολογία θα πρέπει να συλλέγει και να συσχετίζει όλους άλλης τύπους δεδομένων, άλλης κυκλοφορία δικτύου (NTA), αρχεία καταγραφής, εντολές διακομιστή, διεργασίες, εφαρμογές, πληροφορίες χρήστη, αρχεία κ.λπ. αυτοματοποιημένα έτσι ώστε το προσωπικό ασφαλείας να μπορεί να λειτουργεί πιο αποτελεσματικά. | ΝΑΙ | | |
| | Το σύστημα να βασίζεται σε λογισμικό που μπορεί να εγκατασταθεί σε εικονικά και περιβάλλοντα νεφοϋπολογιστικής (cloud). | ΝΑΙ | | |
| | Το σύστημα να πρέπει να παρέχει λειτουργικότητα πολλών μισθωτών (multi-tenant). | ΝΑΙ | | |
| | Σε μια εγκατάσταση πολλαπλών tenants, το σύστημα να εκτελεί λειτουργία μηχανικής μάθησης και τεχνητής νοημοσύνης μόνο στα δεδομένα μεμονωμένων tenants. | ΝΑΙ | | |
| | Προκειμένου να διασφαλιστεί η | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | λεπτομερής ανάλυση των δειγμάτων, προσδιορίζοντας άγνωστες επιθέσεις 0-day (zero-day attacks), η μηχανή ανάλυσης πρέπει να είναι σε θέση να αναπαραγάγει την εκτέλεση κακόβουλου λογισμικού σε έναν εξομοιωτή μηχανής που αναπαράγει ένα εικονικό υλικό, συμπεριλαμβανομένης μιας προσομοιωμένης CPU (Sandboxing) . Η προσομοιωμένη CPU θα πρέπει να εκτελεί προσομοίωση κώδικα σε επίπεδο επεξεργαστή, δηλαδή θα πρέπει να εκτελεί απευθείας τον κακόβουλο κώδικα, ο οποίος, ως εκ τούτου, δεν θα πρέπει να εκτελείται στην φυσική CPU, δηλαδή την κεντρική CPU του προσομοιωμένου συστήματος. | | | |
| | Το προστατευμένο περιβάλλον (sandbox) να βασίζεται στην πλήρη εξομοίωση του συστήματος και να ανιχνεύει επιθέσεις πολλαπλών σταδίων (multi-stage attack) όπου η εκμετάλλευση χωρίζεται σε πολλαπλά αντικείμενα | ΝΑΙ | | |
| | Το σύστημα θα παρέχει προηγμένες δυνατότητες συσχέτισης για τον εντοπισμό περιστατικών ασφαλείας όπως: | ΝΑΙ | | |
| | α. Επιθέσεις DDOS (SYN Flood | ΝΑΙ | | |
| | β. Κρούσμα σκουληκιών (warms) | ΝΑΙ | | |
| | γ. Σάρωση θύρας | ΝΑΙ | | |
| | d. Έγχυση SQL | ΝΑΙ | | |
| | e. Βίαιη επίθεση στην υποδομή (Brute Force) | ΝΑΙ | | |
| | Το σύστημα θα προσφέρεται σε WEB GUI με πρωτόκολλο HTTPS | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα θα χρησιμοποιεί αλγόριθμους που βασίζονται στη μηχανική μάθηση. | ΝΑΙ<br>Να αναφερθούν άνω δύο περιπτώσεων χρήσης και αποδεικτικά στοιχεία ότι η εφαρμογή χρησιμοποιεί αλγόριθμους με βάση τη μηχανική μάθηση | | |
| | Το σύστημα θα πρέπει να μπορεί να υποστηρίζει τουλάχιστον 850 χρήστες. | ΝΑΙ<br>Ο μεγαλύτερος αριθμός είναι επιθυμητός | | |
| | Οι Sensors θα πρέπει να υποστηρίζουν ταχύτητα διασύνδεσης δικτύου 1Gbps, 10Gbps | ΝΑΙ | | |
| | Το σύστημα να μπορεί να υποστηρίζει ταυτόχρονα πολλαπλά locations. | ΝΑΙ | | |
| | Το σύστημα να έχει τη δυνατότητα να αναγνωρίζει τα γεγονότα ως μέρος μιας ροής εργασίας (workflow). | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να διαθέτει προσαρμόσιμο widget στον πίνακα ελέγχου | ΝΑΙ | | |
| | Το σύστημα να παρέχει ενσωματωμένο Intelligence Module για συστήματα βάσεων | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | δεδομένων, άλλης MSSQL, MySQL, Azure EventHub | | | |
| | Το σύστημα θα πρέπει να ενσωματώνεται με τουλάχιστον πέντε ανοιχτές πηγές πληροφοριών για απειλές (Open Source Threat Intelligence) | ΝΑΙ<br>Ο μεγαλύτερος αριθμός είναι επιθυμητός | | |
| | Το σύστημα θα πρέπει να έχει μια κύρια κονσόλα διαχείρισης που αποτελείται από ευρετήριο και dashboard | ΝΑΙ | | |
| | Λειτουργία υψηλής διαθεσιμότητας και ομαδοποίηση. | ΝΑΙ<br>Να αναφερθεί ο βαθμός διαθεσιμότητας | | |
| | Το σύστημα θα πρέπει να παρέχει απόλυτη προστασία από επιθέσεις APT μέσω δικτύου και web. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να υποστηρίζει ειδοποιήσεις συμβάντος (event notification) σε μορφή JSON. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι ικανό να κατηγοριοποιεί την σοβαρότητα συμβάντων (Incident Severity) που συνδέεται με Ειδοποιήσεις. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να έχει τη δυνατότητα να αναφέρει πότε εμφανίζεται DATA THEFT περιστατικό. | ΝΑΙ | | |
| | θα πρέπει να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης αρχιτεκτονικής σε τυπικούς διακομιστές και όχι σε ειδικές συσκευές. | ΝΑΙ<br>Να αναφερθούν οι συμβατοί τύποι διακομιστών | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα πρέπει θα είναι σε θέση να εφαρμόζει τόσο Εποπτευόμενη όσο και Μη Εποπτευόμενη Μηχανική Μάθηση και Προσαρμοσμένη Μηχανική Μάθηση σε αρχεία καταγραφής ή επισκεψιμότητα που λαμβάνει δεδομένα από τα ακόλουθα στοιχεια του δικτύου:<br>IDS<br>Τείχος προστασίας<br>Traffic δικτύου (Network Traffic)<br>Συστήματα Windows ή Linux<br>AWS Cloudtrail, Office 365, G-Suite, SNMP,<br>Vulnerability Scanners όπως Nessus, Rapid7, Tenable<br>Syslogs, CEF, LEEF, Netflow, JSON | ΝΑΙ<br>Να αναφερθούν τα χαρακτηριστικά των χρησιμοποιούμενων μεθόδων Μηχανικής Μάθησης | | |
| | Το σύστημα θα έχει τη δυνατότητα εφαρμογής Μηχανικής Εκμάθησης στο Τείχος προστασίας και τα IDS (ML-IDS) | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει πολλαπλούς μηχανισμούς συλλογής δεδομένων, συμπεριλαμβανομένων αισθητήρων ασφάλειας δικτύου (Network Security Sensors) και Agent Sensors. | ΝΑΙ<br>Να αναφερθούν τα χαρακτηριστικά των αισθητήρων | | |
| | Το σύστημα να παρέχει στον διαχειριστή υπηρεσίες για την εφαρμογή συνεχούς απεριόριστης ενημέρωσης σε dashboard | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να εξαγάγει αναγνώσιμα μεταδεδομένα (layers 2-7) | ΝΑΙ | | |
| | Οι αισθητήρες του συστήματος να καταγράφουν δεδομένα του δικτύου και να αποστέλνουν μόνο σχετικά δεδομένα στον επεξεργαστή για ανάλυση. | ΝΑΙ | | |
| | Το σύστημα θα παρέχει ολοκληρωμένη ανάλυση κίνησης δικτύου (NTA). | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα να παρέχει τεχνολογία εξαπάτησης / honeypot με υποστήριξη τουλάχιστον 2 κοινών πρωτοκόλλων (π.χ. HTTP/FTP) | ΝΑΙ<br>Να αναφερθεί η διαδικασία άλλης εξαπάτησης | | |
| | Το προτεινόμενο σύστημα να είναι ικανό να υποστηρίζει τη συλλογή πληροφοριών και δεδομένων τόσο με τη χρήση agents όσο και χωρίς. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί παρακολούθηση άλλης υποδομής διακομιστή και Δικτύου out of the box. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί την Παρακολούθηση Εφαρμογών out of the box. | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει αναζήτηση γεωγραφικής τοποθεσίας IP (Geo Location Public IP look up) | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει προσαρμοσμένα και εσωτερικά αρχεία καταγραφής ασφαλείας και on-the-fly δημιουργία συσχέτισης για τα αρχεία καταγραφής | ΝΑΙ | | |
| | Το σύστημα να μπορεί να συλλέγει πληροφορίες στοιχείων (network assets) και πληροφορίες ροής δικτύου (network flows) με παθητικό τρόπο (passive) | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να απορροφήσει όλα τα δεδομένα (χρήστες, εφαρμογές) και να τα καταστήσει διαθέσιμα για χρήση — παρακολούθηση, ειδοποίηση, έρευνα και ad hoc αναζήτηση | ΝΑΙ | | |
| | Το σύστημα θα παρέχει ευελιξία για ενσωμάτωση με εργαλεία και πύλες αναφοράς τρίτων | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα να παρέχει δυνατότητα προβολής για αποθηκευμένα ακατέργαστα δεδομένα (raw data view) | ΝΑΙ | | |
| | Το σύστημα να κατατάσσει ειδοποιήσεις ασφαλείας με βάση το CyberSecurity KillChain. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να παρέχει περιγραφή του κακόβουλου λογισμικού που εντοπίστηκε. | ΝΑΙ | | |
| | Το σύστημα να παρέχει ένα ολοκληρωμένο σύστημα ανίχνευση εισβολής (IDS). | ΝΑΙ | | |
| | Το σύστημα να αποστέλλει ειδοποίηση στο αντίστοιχο προσωπικό σχετικά με το ζήτημα ασφάλειας βάσει συσχετισμένου συμβάντος. | ΝΑΙ | | |
| | Το σύστημα να παρακολουθεί κάθε αλλαγή και να προστατεύει το περιβάλλον παρακολουθώντας ύποπτη δραστηριότητα, αλλαγές ρόλου χρήστη, μη εξουσιοδοτημένη πρόσβαση και άλλα. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι σε θέση να εντοπίσει παραβιασμένους κεντρικούς υπολογιστές που σχετίζονται με προηγμένες απειλές και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να παρέχει δυνατότητα παρακολούθησης συμβάντων ασφαλείας εκτός δεδομένων υπολογιστή (π.χ. παρακολούθηση συμβάντων / απειλών ασφαλείας που έχουν αναρτηθεί στο Διαδίκτυο) | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι σε θέση να βρει δραστηριότητες και συμβάντα που σχετίζονται με επιτυχείς επιθέσεις και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα θα πρέπει να παράγει ειδοποίηση κατά τον εντοπισμό εξωτερικής IP που ανήκει σε μαύρη λίστα (blacklist) | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να περιλαμβάνει ενσωματωμένη διαχείριση ειδοποιήσεων για νέα κακόβουλα συμβάντα | ΝΑΙ | | |
| | Το σύστημα να παρέχει ορατότητα δικτύου (network visibility) από wire data που περιέχουν κρίσιμες πληροφορίες για payload, πληροφορίες συνεδρίας (session information), σφάλματα, DNS κ.λπ. | ΝΑΙ | | |
| | Το σύστημα να παρέχει δυνατότητες ανίχνευσης χωρίς χρήση υπογραφών (Signatureless Detection Capability). | ΝΑΙ | | |
| | Το σύστημα να έχει δυνατότητες ανάλυσης συμπεριφοράς χρήστη (User Behavior Analytics) | ΝΑΙ | | |
| | Το σύστημα να έχει δυνατότητες ανάλυσης συμπεριφοράς τερματικών (EndPoint Behavior Analytics) | ΝΑΙ | | |
| | Το σύστημα να έχει προ-εγκατεστημένους κανόνες ανίχνευσης που βασίζονται στο CyberSecurity KillChain | ΝΑΙ | | |
| | Να υποστηρίζει αναζήτηση βάσει ανάλυσης καταγραφής και να εκδίδεται αναφορά. | ΝΑΙ | | |
| | Να πραγματοποιείται ανάλυση και συσχέτιση συμβάντων ασφαλείας. | ΝΑΙ | | |
| | Το σύστημα έρευνας να προσφέρει διαχείριση ολοκληρωμένων απειλών, συμβάντων και συμμόρφωσης | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να καλύψει ιδιωτικά δεδομένα (π.χ. κωδικό πρόσβασης, αριθμό πιστωτικής κάρτας) πριν τα αποθηκεύσει. | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα να παρακολουθεί αυτόματα τα γνωστά κακόβουλα γεγονότα και να χρησιμοποιεί εξελιγμένη συσχέτιση μέσω αναζήτησης, για να εντοπίσει γνωστά μοτίβα κινδύνου άλλης επιθέσεις brute force, διαρροή δεδομένων και ακόμη και απάτη σε επίπεδο εφαρμογής (application-level fraud). | ΝΑΙ | | |
| | Το σύστημα να  είναι σε θέση να βοηθήσει  αναλυτές ασφαλείας να διενεργήσουν αξιολόγηση παραβίασης και ρηγμάτων (compromise and breach assessments). | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να συσχετίζει πληροφορίες στοιχείων (asset info) με δεδομένα απειλών (threat) και ευπαθειών(vulnerability) | ΝΑΙ | | |
| | Το σύστημα να είναι πλήρως προσαρμόσιμο στη δημιουργία προειδοποιήσεων ή συναγερμών για συμβάντα υψηλού κινδύνου | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να παρέχει λειτουργία αναζήτησης που θα υποστηρίζει απλή αναζήτηση μοτίβων τύπου Boolean καθώς και σύνθετες κανονικές εκφράσεις (Boolean-style patterns search as well as complex regular expressions). | ΝΑΙ | | |
| | Το σύστημα να μπορεί να επιτρέπει στον αναλυτή να δημιουργεί ερωτήματα χρησιμοποιώντας συνδυασμένη μέθοδο αναζήτησης. Ένα μεμονωμένο ερώτημα μπορεί να περιέχει λέξεις-κλειδιά, συνθήκες βάσει πεδίου και κανονικές εκφράσεις (keywords, field based conditions and regular expression). | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα να υποστηρίζει τη δυνατότητα σύνδεσης με Threat Intelligence για έκτακτο συμβάν ή και ειδοποίηση. | ΝΑΙ | | |
| | Το σύστημα να μπορεί να ανιχνεύει απειλές που στοχεύουν διάφορα λειτουργικά συστήματα. | ΝΑΙ | | |
| | Το σύστημα να προσφέρει δυνατότητα εγκατάστασης αισθητήρα/agent σε εικονικό περιβάλλον (virtualization) | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να παρέχει συσχέτιση συμβάντων από πολλούς τύπους συσκευών. | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει κοινή χρήση πληροφοριών όπου απαιτείται (community based intel sharing). | ΝΑΙ | | |
| | Το σύστημα να παρέχει ανάλυση κατ ‘απαίτηση για IP και Domains. | ΝΑΙ | | |
| | Το σύστημα να μπορεί ενσωματωθεί με σύστημα ασφάλειας SIEM μέσω προσαρμογέα πληροφοριών ασφαλείας και άλλης εφαρμογής. | ΝΑΙ | | |
| | Το σύστημα να έχει δυνατότητα αξιοποίησης, ανάλυσης και οπτικοποίησης των δεδομένων στον ανοικτού κώδικα Kibana με ενεργοποίηση Plugin. | ΝΑΙ | | |
| | Το σύστημα να παρέχει δυνατότητες ενορχήστρωσης άλλης αυτοματοποίησης απόκρισης ασφάλειας (SOAR) σε email, διαχείριση υποθέσεων (case management), τείχους προστασίας (firewall) και Active Directory | ΝΑΙ | | |
| | Η λειτουργία SIEM να μεταδίδει άλλης ροές συμβάντων και άλλης ανιχνεύσεις SOAR για την αυτόματη ενεργοποίηση πληροφοριών που βρίσκονται σε προϊόντα ενορχήστρωσης SOAR, για την εκτέλεση σειράς οδηγιών | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | που θα μπορούσαν να περιλαμβάνουν την εκτέλεση σεναρίων(playbooks) ή την ενσωμάτωση με άλλα εργαλεία στο ίδιο περιβάλλον. | | | |
| | Το σύστημα να έχει τη δυνατότητα να εντοπίζει και να αυτοματοποιεί την παρακολούθηση απειλής (Threat Hunting) και να εφαρμόζεται στο SOAR | ΝΑΙ | | |
| | Το σύστημα να παρέχει ενσωματωμένη διαχείριση υποθέσεων (case management) ή να μπορεί να συνδεθεί με διαχείριση συμβάντων (case management) άλλων συστημάτων | ΝΑΙ | | |
| | Το σύστημα να έχει ήδη προκαθορισμένα πρότυπα για γενικές αναφορές και αναφορές συμμόρφωσης (general and compliance reporting) | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι σε θέση να συλλέγει ποσότητες δεδομένων χωρίς να περιορίζει τον αριθμό των συσκευών από άλλης οποίες θα πρέπει να συλλέγονται. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να παρέχει απεριόριστο όριο στον αριθμό των χρηστών στο σύστημα, αναζητήσεις, ειδοποιήσεις, συσχετίσεις, αναφορές, πίνακες ελέγχου. | ΝΑΙ | | |
| | Συλλέγει όλους άλλης τύπους αρχείων καταγραφής και δεδομένων από διάφορες πηγές, π.χ. syslog, προσαρμοσμένες / εσωτερικές εφαρμογές και αρχεία καταγραφής βάσεων δεδομένων | ΝΑΙ | | |
| | Ενοποιεί όλα τα συλλεγόμενα αρχείων καταγραφής σε ένα κεντρικό αποθετήριο. | ΝΑΙ | | |
| | Εκτελεί συγκέντρωση και ομαλοποίηση αρχείων | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | καταγραφής. | | | |
| | Αναλύει και να συσχετίζει τα συμβάντα ασφαλείας. | ΝΑΙ | | |
| | Στέλνει ειδοποίηση στο αντίστοιχο προσωπικό σχετικά με το ζήτημα ασφάλειας βάσει συσχετισμένου συμβάντος. | ΝΑΙ | | |
| | Το σύστημα πρέπει να περιλαμβάνει ενσωματωμένη διαχείριση απειλών, συμβάντων και συμμόρφωσης. | ΝΑΙ | | |
| | Το σύστημα πρέπει να είναι μια λύση βάσει λογισμικού που να μπορεί να εγκατασταθεί σε εικονικά περιβάλλοντα (virtualized environments). | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να περιλαμβάνει αισθητήρα συλλογής δεδομένων | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει τη συλλογή δεδομένων με χρήση ή και χωρίς agent (agent & agentless) | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι ικανό να εκτελεί Παρακολούθηση Εφαρμογών out of the box. | ΝΑΙ | | |
| | Το σύστημα να παρέχει παρακολούθηση αλλαγών και προστασία του περιβάλλοντος του Οργανισμού , παρακολουθώντας ύποπτη δραστηριότητα, αλλαγές ρόλου χρήστη, μη εξουσιοδοτημένη πρόσβαση και άλλα. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να παρακολουθεί αυτόματα την υποδομή για γνωστά κακόβουλα συμβάντα και θα χρησιμοποιεί εξελιγμένη συσχέτιση μέσω αναζήτησης, για να εντοπίσει γνωστά μοτίβα κινδύνου άλλης επιθέσεις με ωμή βία (brute-force attack), διαρροή δεδομένων (data | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | leakage) και ακόμη και απάτη σε επίπεδο εφαρμογής (application level fraud). | | | |
| | Το σύστημα να  είναι σε θέση να εντοπίσει παραβιασμένους κεντρικούς υπολογιστές που σχετίζονται με προηγμένες απειλές και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να εντοπίζει δραστηριότητες και συμβάντα που σχετίζονται με επιτυχείς επιθέσεις και μολύνσεις από κακόβουλα προγράμματα | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να βοηθήσει άλλης αναλυτές ασφαλείας να διενεργήσουν διερεύνηση εισβολών και ρηγμάτων (compromise and breach assessment). | ΝΑΙ | | |
| | Να παρέχει τη δυνατότητα παρακολούθησης συμβάντων ασφαλείας εκτός δεδομένων υπολογιστή (π.χ. παρακολούθηση συμβάντων / απειλών ασφαλείας που έχουν αναρτηθεί στο Διαδίκτυο) | ΝΑΙ | | |
| | Να υποστηρίζει προσαρμοσμένα και εσωτερικά αρχείων καταγραφής ασφαλείας και την on-the-fly συσχετισμό άλλης. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να υποστηρίζει ενσωμάτωση με μηχανισμούς αναγνώρισης ευπαθειών (vulnerability scanners) | ΝΑΙ | | |
| | Το σύστημα θα είναι σε θέση να συσχετίζει πληροφορίες στοιχείων (assets) με δεδομένα απειλής και ευπάθειας | ΝΑΙ | | |
| | Το σύστημα να μπορεί να συλλέγει παθητικά (passively) πληροφορίες στοιχείων (assets) και πληροφορίες ροής δικτύου (network flow) | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα θα πρέπει να υποστηρίζει προβολή για αποθηκευμένα ακατέργαστα δεδομένα | ΝΑΙ | | |
| | Το σύστημα να μπορεί να εκδίδει ειδοποίηση κατά τον εντοπισμό εξωτερικής IP μαύρης λίστας | ΝΑΙ | | |
| | Το σύστημα να μπορεί να ενοποιήσει άλλης απειλές με την ομαλοποίηση (normalization) , τη φήμη (reputation), τη γνώση (knowledge) και payload του γεγονότος ενεργοποίησης | ΝΑΙ | | |
| | Το σύστημα να παρέχει λειτουργία network packet analysis για διαγνωστικό έλεγχο. | ΝΑΙ | | |
| | Το σύστημα να είναι πλήρως παραμετροποιήσιμο κατά τη δημιουργία προειδοποιήσεων (warnings) ή συναγερμών (alarms) για συμβάντα υψηλού κινδύνου | ΝΑΙ | | |
| | Το σύστημα να παρέχει ορατότητα δικτύου (network visibility) από wire data που περιέχουν κρίσιμες πληροφορίες για payload, πληροφορίες περιόδου λειτουργίας (session information), σφάλματα, DNS κ.λπ. | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να παρέχει λειτουργία αναζήτησης που θα υποστηρίζει απλή αναζήτηση μοτίβων τύπου Boolean καθώς και σύνθετες κανονικές εκφράσεις (Boolean-style patterns search και complex regular expressions). | ΝΑΙ | | |
| | Το σύστημα να μπορεί να επιτρέπει στον αναλυτή να δημιουργεί ερωτήματα (queries) χρησιμοποιώντας συνδυασμένη μέθοδο αναζήτησης. Ένα μεμονωμένο ερώτημα μπορεί να περιέχει λέξεις-κλειδιά, συνθήκες βάσει πεδίου και κανονικές | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | εκφράσεις (keywords, field based conditions and regular expression). | | | |
| | Το σύστημα να είναι σε θέση να εκτελεί υπο-αναζήτηση όσον αφορά την ασφάλεια στα αποτελέσματα τρέχουσας αναζήτησης | ΝΑΙ | | |
| | Το σύστημα να μπορεί να παρακολουθεί άγνωστες απειλές | ΝΑΙ | | |
| | Το σύστημα να παρέχει οπτικές αναφορές που μπορούν να μεταφράσουν τα ζητήματα ασφαλείας σε επιχειρηματικό κίνδυνο / απώλεια και αντίκτυπο (risk/loss and impact). | ΝΑΙ | | |
| | Το σύστημα να  είναι σε θέση να απορροφήσει όλα τα δεδομένα (χρήστες, εφαρμογές) και να τα καταστήσει διαθέσιμα για χρήση — παρακολούθηση, ειδοποίηση, έρευνα, ad hoc αναζήτηση | ΝΑΙ | | |
| | Το σύστημα να παρέχει είναι ένα διαδικτυακό WEB GUI με πρωτόκολλο HTTPS | ΝΑΙ | | |
| | Το σύστημα να  παρέχει ευελιξία για ενσωμάτωση με εργαλεία και πύλες αναφοράς τρίτων | ΝΑΙ | | |
| | Το σύστημα θα χρησιμοποιεί αλγόριθμους που βασίζονται στη μηχανική μάθηση. Καταχωρίστε ορισμένες περιπτώσεις χρήσης και αποδεικτικά στοιχεία ότι η εφαρμογή χρησιμοποιεί αλγόριθμους με βάση τη μηχανική μάθηση | ΝΑΙ | | |
| | Το σύστημα να παρέχει ενσωμάτωση με advanced security advisory | ΝΑΙ | | |
| | Το σύστημα να παρέχει υποστήριξη για ενοποίηση δεδομένων υποστήριξης για την ανάλυση του κινδύνου (Risk Analytic data integration) | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Το σύστημα να παρέχει υποστήριξη για ενημερώσεις κινδύνου και απειλών στον κυβερνοχώρο (Risk and Cyber Threat Advisory Alert) | ΝΑΙ | | |
| | Το σύστημα θα πρέπει παρέχει στον διαχειριστή την δυνατότητα συνεχούς, απεριόριστης ενημέρωσης του πίνακα ελέγχου (dashboard) και των ερωτημάτων συσχέτισης | ΝΑΙ | | |
| | Το σύστημα θα παρέχει προεγκατεστημένο Intelligence Module, πλαίσιο λειτουργίας (dashboard) και αναφορών για τα Windows | ΝΑΙ | | |
| | Να διαθέτει αισθητήρα/λειτουργία υψηλής διαθεσιμότητας | ΝΑΙ | | |
| | Το σύστημα να διαθέτει ενότητα ανάλυσης επιχειρησιακής ευφυίας (Intelligent business analysis module) | ΝΑΙ | | |
| | Το σύστημα να διαθέτει συμβουλευτική ενότητα αξιολόγησης ρίσκου και συμμόρφωσης (risk and compliance advisory module) | ΝΑΙ | | |
| | Το σύστημα να παρέχει προστασία από επιθέσεις APT μέσω δικτύου ή Web | ΝΑΙ | | |
| | Το σύστημα να παρέχει άλλης δυνατότητες ανίχνευσης χωρίς σήμανση (Signatureless Detection). | ΝΑΙ | | |
| | Το σύστημα να μπορεί να υποστηρίζει SNMP. | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να αντιμετωπίσει όλους άλλης τύπους ειδοποιήσεων που συνδέονται με άλλης φάσεις του κύκλου ζωής άλλης μόλυνσης (Infection Life Cycle). | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να είναι ικανό να κατηγοριοποιήσει άλλης | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | ειδοποιήσεις με βάση τη σοβαρότητα (Incident Severity). | | | |
| | θα πρέπει να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης αρχιτεκτονικής σε τυπικούς διακομιστές του εμπορίου και όχι σε ειδικές συσκευές. | ΝΑΙ | | |
| | Το σύστημα θα υποστηρίζει τη δυνατότητα σύνδεσης ειδοποιήσεων/συμβάντων με Threat Intelligence. | ΝΑΙ | | |
| | Το σύστημα να μπορεί να ανιχνεύει απειλές που στοχεύουν διάφορα λειτουργικά συστήματα. | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει Διαμόρφωση Υψηλής Διαθεσιμότητας (HA). Να αναφερθεί | ΝΑΙ | | |
| | Το σύστημα να είναι σε θέση να παρέχει συσχέτιση συμβάντων από πολλούς τύπους συσκευών. | ΝΑΙ | | |
| | Το σύστημα θα περιλαμβάνει ενοποιημένες λήψεις περιεχομένου ασφαλείας για άλλης διαχειριζόμενες συσκευές. | ΝΑΙ | | |
| | Το σύστημα να υποστηρίζει κοινή χρήση πληροφοριών. | ΝΑΙ | | |
| | Το σύστημα να παρέχει δημιουργία ειδοποιήσεων για γνωστούς παράγοντες απειλής (attribution of alerts to known threat actors). | ΝΑΙ | | |
| | Το σύστημα να παρέχει περιγραφή άλλης οικογένειας των κακόβουλων προγραμμάτων. | ΝΑΙ | | |
| | Το σύστημα να παρέχει ανάλυση κατ ‘απαίτηση για IP και Domains. | ΝΑΙ | | |
| | Το σύστημα θα πρέπει να ενσωματωθεί με το σύστημα ασφάλειας SIEM. | ΝΑΙ | | |
| | Να είναι δυνατή η εγκατάσταση του αισθητήρα/agent σε εικονικό περιβάλλον | ΝΑΙ | | |
| | Να είναι δυνατή η εγκατάσταση όλων των στοιχείων άλλης | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | αρχιτεκτονικής σε τυπικούς διακομιστές | | | |
| | Το IDS θα πρέπει να συνδυάζει την τεχνητή νοημοσύνη και υπογραφές για την μείωση των περιττών ειδοποιήσεων/συμβάντων και τον εντοπισμό ανωμαλιών υψηλής πιστότητας | ΝΑΙ | | |
| | Η αρχιτεκτονική θα πρέπει να παρέχει εκτεταμένη ανάλυση κίνησης δικτύου χρησιμοποιώντας τόσο εποπτευόμενη όσο και μη εποπτευόμενη μάθηση | ΝΑΙ | | |
| | Θα πρέπει να παρέχει παρακολούθηση άλλης αλληλεπίδρασης μεταξύ συσκευών, υπηρεσιών, εφαρμογών που εκτελούνται στο δίκτυό σε πραγματικό χρόνο όσο και ιστορικά. | ΝΑΙ | | |
| | Στατιστικά στοιχεία απόδοσης δικτύου (Network Statistics) | ΝΑΙ | | |
| | Απόδοση διακομιστών (Server Performance) | ΝΑΙ | | |
| | Ανίχνευση εφαρμογών και παρακολούθηση απόδοσης (Application detection and performance monitoring) | ΝΑΙ | | |
| | Κορυφαίες πηγές και κορυφαίοι προορισμοί (Top sources & Top destinations) | ΝΑΙ | | |
| | Asset throughput | ΝΑΙ | | |
| | Asset application performance | ΝΑΙ | | |
| | Application processing time | ΝΑΙ | | |
| | Network interactions with asset | ΝΑΙ | | |
| | Στατιστικά HTTP | ΝΑΙ | | |
| | Στατιστικά DNS | ΝΑΙ | | |
| | διεύθυνση IP | ΝΑΙ | | |

| Α/Α | ΠΕΡΙΓΡΑΦΗ | ΑΠΑΙΤΗΣΗ | ΑΠΑΝΤΗΣΗ | ΠΑΡΑΠΟΜΠΗ |
|---|---|---|---|---|
| | Υπηρεσίες Εφαρμογών (Application Services)<br>Πρώτη και τελευταία εμφάνιση<br>Ετικέτες και περιγραφή στοιχείων<br>Server certificate visibility. | ΝΑΙ | | |
| | Θα πρέπει να παρέχει εξομοιώσεις (emulations) και δολώματα (decoys) που εκτελούνται στον Deception Server:<br>Διακομιστή HTTP Apache<br>Διακομιστή FTP<br>Διακομιστή SSH<br>Διακομιστή αστερίσκου (VOIP)<br>Διακομιστή Tomcat<br>Πρόσθετο Strut2<br>Διακομιστή SQL | ΝΑΙ | | |
| | Επανεξέταση ελέγχου συστήματος (System auditing) | ΝΑΙ | | |

**Γούρνες, 04 - 05 - 2023**

| | | |
|---|---|---|
| **ΣΥΝΤΑΧΘΗΚΕ**<br><br>**Αθανάσιος Σακκούδης** | | **ΘΕΩΡΗΘΗΚΕ**<br>**Ο Δντης Διοικητικών Υπηρεσιών**<br><br>**Νικόλαος Βασιλάκης** |