ΕΡΓΟ ΠΟΥ ΑΦΟΡΑ
ΤΟΝ ΣΧΕΔΙΑΣΜΟ , ΠΡΟΜΗΘΕΙΑ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ, ΛΟΓΙΣΜΙΚΟΥ ΣΥΛΛΟΓΗΣ, ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ (SIEM – SECURITY INFORMATION AND EVENT MANAGEMENT)

Ελάχιστες Προϋποθέσεις

Ο Ανάδοχος θα πρέπει να διαθέτει σύστημα διαχείρισης της ασφάλειας πληροφοριών σύμφωνα με το διεθνές πρότυπο ISO/IEC 27001:2005.

ΚΕΦΑΛΑΙΟ 1

1.1.Τεχνική Περιγραφή

Το προσφερόμενο λογισμικό διαχείρισης των περιστατικών ασφαλείας θα πρέπει να αποτελεί μια **ολοκληρωμένη**, **αξιόπιστη** και **επεκτάσιμη υποδομή διαχείρισης και ανάλυσης περιστατικών ασφαλείας** για τα πληροφοριακά συστήματα και τις εφαρμογές της Βουλή των Ελλήνων.

Το λογισμικό αυτό θα εγκατασταθεί σε περιβάλλον VMWare και θα πρέπει να αποτελείται από ένα σύστημα συλλογής μεγάλου όγκου δεδομένων αναφορών (Logs, events κτλ.), αποθήκευσης, κατηγοριοποίησης, και ανάλυσης αυτών σε πραγματικό χρόνο.

Επίσης θα πρέπει να παρέχεται η δυνατότητα ενημέρωσης των διαχειριστών βάσει κανόνων όπως περιπτώσεις προσπαθειών παραβίασης της ασφάλειας, καθώς και η δημιουργία αναφορών για λόγους υποστήριξης με ρυθμιστικές πρωτοβουλίες συμμόρφωσης και ελέγχων από εξωτερικούς παράγοντες (auditing).
Θα πρέπει να υπάρχει η δυνατότητα ανάλυσης των δεδομένων βάσει συσχετισμών από

α) διαφορετικές πηγές
β) διαφορετική ώρα

Το προσφερόμενο σύστημα θα πρέπει να χρησιμοποιηθεί ως το κεντρικό σημείο διαχείρισης / ανάλυσης logs της Βουλή των Ελλήνων και θα πρέπει να παρέχει τα τεχνικά χαρακτηριστικά και τις δυνατότητες δημιουργίας, διαχείρισης και αποθήκευσης κεντρικοποιήμενης πολιτικής συλλογής / ανάλυσης / και ενημέρωσης (alerting) σε πραγματικός χρόνο.
Η πρόσβαση στο σύστημα θα πρέπει να βασίζεται σε ρόλους (role based access control).

Οι λεπτομερείς προδιαγραφές του συστήματος τις οποίες πρέπει να ακολουθήσει ο Ανάδοχος βρίσκονται στο Παράρτημα 1.

1.2. Επιπλέον χαρακτηριστικά

1.2.1 Διαλειτουργικότητα

Το ολοκληρωμένο σύστημα πρέπει υποχρεωτικά να σχεδιαστεί και να υλοποιηθεί έτσι, ώστε να διασφαλιστεί η επικοινωνία (συλλογής δεδομένων) με τα υφιστάμενα αλλά και μελλοντικά συστήματα / εφαρμογές της Βουλής των Ελλήνων.

Στο πλαίσιο του παρόντος έργου είναι απαραίτητη η διασφάλιση της επικοινωνίας με τα ακόλουθα συστήματα:

- ✓ Σύστημα Windows (Servers, Desktops- αν χρειαστεί),
- ✓ Σύστημα AIX
- ✓ Βάσεις Δεδομένων SQL – DB2 – Oracle
- ✓ Web Servers (Apache, IIS κτλ)
- ✓ Δικτυακό εξοπλισμό (Cisco routers, switches, wireless APs)
- ✓ Flat files – text files
- ✓ Checkpoint Firewalls
- ✓ Web Filtering
- ✓ Proxy
- ✓ Antivirus
- ✓ Εφαρμογές (Εσωτερικές ή εμπορικές)

Να αναφερθούν τα πρότυπα και οι τεχνολογίες με τις οποίες επιτυγχάνεται η επικοινωνία με τα υφιστάμενα αλλά και μελλοντικά συστήματα.

1.2.2. Ασφάλεια

Κατά το σχεδιασμό του Έργου ο Ανάδοχος θα πρέπει να λάβει ειδική μέριμνα και να δρομολογήσει τις κατάλληλες δράσεις για:

- ✓ την Ασφάλεια του συστήματος που προδιαγράφει το παρόν Έργο,
- ✓ την προστασία της ακεραιότητας και της διαθεσιμότητας των πληροφοριών,
- ✓ την προστασία των προς επεξεργασία και αποθηκευμένων προσωπικών δεδομένων, αναζητώντας και εντοπίζοντας με μεθοδικό τρόπο τα τεχνικά μέτρα και τις οργανωτικές και

διοικητικές διαδικασίες, οι οποίες είναι αναγκαίες για την επαρκή ασφάλεια του πληροφοριακού συστήματος.

Για το σχεδιασμό και την υλοποίηση των τεχνικών μέτρων ασφαλείας του Έργου, ο Ανάδοχος πρέπει να λάβει υπόψη του:

- ✓ *τις σύγχρονες εξελίξεις στις ΤΠΕ,*
- ✓ *τις βέλτιστες πρακτικές στο χώρο της Ασφάλειας στις ΤΠΕ (best practices),*
- ✓ *τυχόν διεθνή de facto ή de jure σχετικά πρότυπα.*

Προκειμένου να επιτευχθεί ο μέγιστος δυνατός βαθμός προστασίας του πληροφοριακού συστήματος, απαιτούνται κατ' ελάχιστο τα εξής:

Τεχνικά Μέτρα Ασφάλειας (Security Safeguards-Countermeasures).

Ο Ανάδοχος είναι υποχρεωμένος να υποβάλει, **ως παραδοτέο**, Σχέδιο Τεχνικής Ασφάλειας του Συστήματος.

Το σχέδιο θα πρέπει να καλύπτει τεχνικά θέματα ασφάλειας του υπολογιστικού εξοπλισμού, των δεδομένων του συστήματος και του λογισμικού που θα εγκατασταθεί.

Η τεχνική προσφορά του Αναδόχου θα πρέπει να περιγράφει τη συνολική τεχνική μεθοδολογική προσέγγιση για την υλοποίηση ενός τεχνικά ασφαλούς πληροφοριακού συστήματος.

Κεφάλαιο 2 ΜΕΘΟΔΟΛΟΓΙΑ ΦΑΣΕΩΝ ΥΛΟΠΟΙΗΣΗΣ ΤΟΥ ΕΡΓΟΥ

2.1 ΦΑΣΕΙΣ Υλοποίησης του Έργου

2.1.1 .Μελέτη Εφαρμογής

Ο Ανάδοχος θα πρέπει να εκπονήσει και να παραδώσει τη **Μελέτη Εφαρμογής**. Μέσα από αυτήν την ανάλυση, θα εξαχθούν οι λεπτομερείς προδιαγραφές για το σύστημα διαχείρισης των περιστατικών ασφαλείας.

Η **Μελέτη Εφαρμογής** θα συνιστά τον «οδηγό υλοποίησης» και τη βάση αναφοράς για την παρακολούθηση της προόδου των εργασιών καθ' όλη την διάρκεια του Έργου και περιλαμβάνει τα εξής:

- **Σχέδιο Διαχείρισης και Ποιότητας Έργου (ΣΔΠΕ)**. Οι διαδικασίες και μηχανισμοί που θα περιγράφονται αναλυτικά στο Σχέδιο θα πρέπει να αποτελούν ένα πρότυπο και ολοκληρωμένο σύνολο, προσαρμοσμένο στις ιδιαιτερότητες που θέτουν οι οργανωτικοί, διοικητικοί και τεχνολογικοί παράμετροι του έργου.

  Με βάση τα παραπάνω, τα περιεχόμενα του ΣΔΠΕ θα πρέπει κατ' ελάχιστο να αναφέρονται στις ακόλουθες περιοχές των οποίων ο σκοπός, η δομή και το περιεχόμενο θα περιγράφεται αναλυτικά στην προσφορά του Αναδόχου:

  - ✓ *Οργανωτικό Σχήμα/ Δομή Διοίκησης Έργου*
  - ✓ *Σχέδιο Επικοινωνίας*
  - ✓ *Προγραμματισμός Έργου*
  - ✓ *Διαχείριση Θεμάτων*
  - ✓ *Εκτίμηση - Διαχείριση Κινδύνων*
  - ✓ *Διασφάλιση – Έλεγχος Ποιότητας*
  - ✓ *Διαχείριση Αρχείων - Δεδομένων*
  - ✓ *Διαχείριση Αλλαγών*
  - ✓ *Διοικητική Πληροφόρηση.*
- **Επικαιροποίηση** της υφιστάμενης κατάστασης.
- **Οριστικοποίηση-ιεράρχηση** των Επιχειρησιακών, Λειτουργικών και Τεχνικών Απαιτήσεων του Έργου καθώς και οριοθέτηση-αποσαφήνιση του εύρους του Έργου,
- **Σχηματική αποτύπωση και τεκμηρίωση** της προτεινόμενης αρχιτεκτονικής προσέγγισης του Υποψηφίου Αναδόχου, σύμφωνα με τις απαιτήσεις του Έργου, και βέλτιστες διεθνείς πρακτικές και τυποποιήσεις.
- **Μεθοδολογία ελέγχου αποδοχής** όπου θα καθορίζονται προδιαγραφές και χρονοδιαγράμματα για τα σενάρια δοκιμής των επιμέρους υποσυστημάτων ως ολότητα, με

σαφή αναφορά στα δεδομένα δοκιμής και καθορισμό της/των μεθόδων καταγραφής των δεικτών απόδοσης της εφαρμογής. Καταγραφή διαδικασία για τις δοκιμές ελέγχου που θα γίνουν στο πλαίσιο των σχετικών παραλαβών. Κατ' ελάχιστο θα πρέπει να προβλέπονται εκτελέσεις αυτοματοποιημένων δοκιμών μονάδων (unit tests), δοκιμών σε επίπεδο λογισμικού (system tests), δοκιμών αποδοχής χρηστών (user acceptance tests)

- **Μεθοδολογία, πρόγραμμα και προδιαγραφές** για το υλικό της εκπαίδευσης των χρηστών.
- **Ανάπτυξη Σχεδίου Ασφάλειας**

Μελέτη Εφαρμογής -	
Παραδοτέα (ελάχιστα):	
1	**Σχέδιο Διαχείρισης και Ποιότητας Έργου (ΣΔΠΕ)**
2	**Οριστικοποιημένο Τεύχος Ανάλυσης Απαιτήσεων**
3	**Σχεδιασμός Αρχιτεκτονικής λύσης (Technical Architecture & Conceptual Design)**
4	**Σχέδιο κατάρτισης /εκπαίδευσης στελεχών Βουλή των Ελλήνων**
5	**Σενάρια και μεθοδολογία ελέγχου**
6	**Μελέτη Αποτίμησης Επικινδυνότητας**
7	**Σχέδιο Ασφάλειας**

2.1.2.Προμήθεια – Εγκατάσταση λογισμικού συστημάτων (Systems S/W)

Ο Ανάδοχος έχει την ευθύνη εγκατάστασης του λογισμικού συστημάτων που υποστηρίζει την ολοκληρωμένη Λύση.
Πιο συγκεκριμένα θα μεριμνήσει για:

- ✓ Παράδοση των προδιαγραφών που θα φιλοξενήσει την λύση, βάση της αρχιτεκτονικής που έχει προαναφερθεί.
- ✓ την εγκατάσταση και ρύθμιση όλου του εξοπλισμού και του απαιτούμενου λογισμικού συστημάτων με εξασφάλιση συμβατότητας με όλη την υπάρχουσα υποδομή

Στο χρονοδιάγραμμα που θα συνοδεύει κάθε προσφορά πρέπει να προκύπτει σαφώς ο χρόνος κατά τον οποίο πρέπει να έχει γίνει η διαμόρφωση του χώρου εγκατάστασης, σε σχέση με την έναρξη του έργου (ημερομηνία υπογραφής της Σύμβασης).

Η προετοιμασία των χώρων για την εγκατάσταση του εξοπλισμού ***δεν είναι υποχρέωση του Αναδόχου.***

Σε περίπτωση προσφοράς που δεν καθορίζει ειδικές συνθήκες περιβάλλοντος θα θεωρηθεί ότι αυτές δεν απαιτούνται ή θα γίνουν με δαπάνη του Αναδόχου.
Ο Ανάδοχος καθορίζει τις λεπτομέρειες σχετικά με τη μεταφορά, τοποθέτηση και εγκατάσταση του λογισμικού και ενημερώνει την Βουλή των Ελλήνων.

2.1.3. Δοκιμές Έλεγχου – Τεκμηρίωση

Για να διαπιστωθεί ότι το έργο ανταποκρίνεται πλήρως στις απαιτήσεις των προδιαγραφών και εκπληρώνει τους σκοπούς για τους οποίους δημιουργήθηκε θα γίνουν έλεγχοι την Αποδοχή του Συστήματος.
Ο Ανάδοχος με την ολοκλήρωση της παράδοσης και εγκατάστασης του εξοπλισμού, και την ολοκλήρωση της παράδοσης και εγκατάστασης του συστήματος υποχρεούται να παραδώσει το σύστημα στο σύνολο του άριστα ελεγμένο.
Για την επίτευξη αυτής της υποχρέωσης, ο ανάδοχος οφείλει να συνεργαστεί με την Interamrican, να διενεργήσει τους ελέγχους και να τεκμηριώσει τα αποτελέσματά τους.
Ο κύκλος Δοκιμών λειτουργικότητας και επίδοσης του Συστήματος θα περιλαμβάνει ενδεικτικά τα ακόλουθα:

- ✓ Δημιουργία πολλαπλών σεναρίων ελέγχου - test plans που θα καλύπτει το πλήρες φάσμα λειτουργίας του Συστήματος (βάσει του Λειτουργικού Σχεδιασμού.
- ✓ Αξιοποίηση όλων των εναρκτήριων παραγωγικών δεδομένων

- ✓ Διεξαγωγή ελέγχων
- ✓ Αποτελέσματα ελέγχων – διορθώσεις & ρυθμίσεις (system tuning), κ.ο.κ

Οι δοκιμές θα εκτελούνται από τον Ανάδοχο μέχρι της απαλοιφής των όποιων ατελειών και της επίτευξης αποδεκτής από τους χρήστες επίδοσης του Συστήματος.
Τα σενάρια ελέγχου διακρίνονται σε :

- ✓ **Unit tests**, με τα οποία θα ελέγχεται και θα επιβεβαιώνεται η λειτουργικότητα και η αποδεκτή επίδοση του Συστήματος.
- ✓ **System - Integration tests** με τα οποία ελέγχεται η συνολική λειτουργικότητα και αποδεκτή επίδοση του Συστήματος.

Η επιτυχής διεξαγωγή των δοκιμών αποδοχής αποτελεί προϋπόθεση για την έναρξη της Πιλοτικής Λειτουργίας.
Τα σενάρια θα καλύπτουν το πλήρες φάσμα της λειτουργικότητας του συστήματος. Οι δοκιμές αποδοχής θα διεξαχθούν σύμφωνα με τα εγκεκριμένα σενάρια. ***Υποχρέωση του Αναδόχου είναι η παροχή του απαραίτητου προσωπικού (τεχνικό και επιχειρησιακό) για την υποστήριξη της διαδικασίας και την διόρθωση / απαλοιφή / τελικές ρυθμίσεις του συστήματος που πιθανόν θα προκύψουν.***

Δοκιμές ελέγχου – τεκμηρίωση	
Παραδοτέα (ελάχιστα):	
1	**Πρόγραμμα Ελέγχου**
2	**Σενάρια Ελέγχου**
3	**Αποτελέσματα Ελέγχου**
4	**Εγχειρίδια κατασκευαστών**

2.1.4.Εκπαίδευση

Οι υπηρεσίες εκπαίδευσης είναι συμπληρωματικές ως προς το βασικό έργο της υλοποίησης του συστήματος και περιλαμβάνονται στις βασικές υποχρεώσεις του Αναδόχου του παρόντος Έργου.
Οι υπηρεσίες εκπαίδευσης θα παρασχεθούν στον χώρο της Βουλή των Ελλήνων.

Στόχος των υπηρεσιών εκπαίδευσης είναι:

- ✓ η ολοκληρωμένη μεταφορά τεχνογνωσίας προς ένα ικανό πυρήνα στελεχών της Βουλή των Ελλήνων, οι οποίοι θα αναλάβουν μετά το πέρας του έργου την διαχείριση, υποστήριξη και περαιτέρω εξέλιξη του συστήματος

- ✓ η επίλυση προβλημάτων που σχετίζονται με την αρχική εξοικείωση των διαχειριστών και τη συστηματική υποστήριξη της προσαρμογής τους στα νέα εργαλεία.

2.1.5.Περίοδος Πιλοτικής Λειτουργίας

Μετά την ολοκλήρωση της υλοποίησης του συστήματος, ο Ανάδοχος πρέπει να θέσει το Σύστημα σε Πιλοτική Λειτουργία.

Η πιλοτική Λειτουργία του συστήματος αναφέρεται στο πρώτο στάδιο της πραγματικής λειτουργίας του συστήματος και θα πρέπει να πραγματοποιηθεί:

- ✓ για το προκαθορισμένο χρονικό διάστημα.
- ✓ με τη συμμετοχή μιας περιορισμένης, αλλά αντιπροσωπευτικής ομάδας χρηστών, καλύπτοντας το σύνολο των λειτουργιών του συστήματος.
- ✓ χρησιμοποιώντας αντιπροσωπευτική πληροφορία για τον ενδελεχή έλεγχο του συστήματος.

Ο Ανάδοχος, κατά την περίοδο της Πιλοτικής Λειτουργίας του Συστήματος, έχει τις παρακάτω υποχρεώσεις:

- ✓ Επίλυση προβλημάτων,
- ✓ Διόρθωση / Διαχείριση λαθών,
- ✓ Υποστήριξη χρηστών με φυσική παρουσία στελεχών του Αναδόχου (συλλογή παρατηρήσεων από τους χρήστες, υποστήριξη στο χειρισμό και λειτουργία των υπολογιστών, εφαρμογών, κλπ.)
- ✓ Υποστήριξη help- desk

Ειδικότερα, στις υποχρεώσεις του Αναδόχου κατά την περίοδο πιλοτικής λειτουργίας είναι να ελεγχθούν διεξοδικά:

- ✓ Οι ρυθμίσεις, παραμετροποιήσεις και προσαρμογές του λογισμικού συστήματος,
- ✓ Η ολοκλήρωση των υλοποιημένων υποσυστημάτων,
- ✓ Οι ρυθμίσεις του συστήματος για τη βελτίωση της απόδοσης (fine tuning).
- ✓ Οποιαδήποτε άλλη παράμετρος επηρεάζει την ομαλή λειτουργία του συστήματος

Σε περίπτωση που κατά την περίοδο Πιλοτικής Λειτουργίας, εμφανισθούν προβλήματα ή διαπιστωθεί ότι δεν πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, ο Ανάδοχος οφείλει να προβαίνει άμεσα στις απαραίτητες βελτιωτικές παρεμβάσεις και αναπροσαρμογές, ώστε το Σύστημα, μετά το πέρας της περιόδου Πιλοτικής Λειτουργίας, να είναι έτοιμο για παραγωγική εκμετάλλευση (deployment).

Επιπλέον, προβλήματα των δεδομένων που ενδεχομένως εμφανιστούν κατά την πιλοτική λειτουργία, θα πρέπει να αντιμετωπιστούν κατάλληλα από τον Ανάδοχο πριν την έναρξη της παραγωγικής λειτουργίας του συστήματος.

2.1.6.Περίοδος Παραγωγικής Λειτουργίας

Η Παραγωγική Λειτουργία του Συστήματος αναφέρεται στην πραγματική λειτουργία του Συστήματος και θα πρέπει να πραγματοποιηθεί:

- ✓ *Για ένα προκαθορισμένο χρονικό διάστημα μετά την λήξη της Πιλοτικής Λειτουργίας του Συστήματος*
- ✓ *Χρησιμοποιώντας το σύνολο του εξοπλισμού του Συστήματος.*
- ✓ *με το σύνολο των χρηστών και για το σύνολο των λειτουργιών του Συστήματος*

Το Σύστημα τίθεται σε πλήρη Παραγωγική Λειτουργία, προκειμένου να λειτουργήσει σε πραγματικές συνθήκες εργασίας

Σε περίπτωση που κατά την περίοδο Παραγωγικής Λειτουργίας, εμφανισθούν σοβαρά προβλήματα ή διαπιστωθεί ότι δεν πληρούνται κάποιες από τις προδιαγραφόμενες απαιτήσεις, ο Ανάδοχος οφείλει να προβαίνει άμεσα στις απαραίτητες βελτιωτικές παρεμβάσεις και αναπροσαρμογές ώστε με το πέρας της περιόδου της Παραγωγικής Λειτουργίας το σύστημα να ικανοποιεί όλες τις απαιτήσεις και προδιαγραφές και να αντικαταστήσει πλήρως το υφιστάμενο χειρόγραφο και μηχανογραφημένο περιβάλλον εργασίας.

2.1.7.Υπηρεσίες Τεχνικής Υποστήριξης

Ο Ανάδοχος υποχρεούται να περιγράψει τις παρεχόμενες Υπηρεσίες Τεχνικής Υποστήριξης, που θα παρέχει καθ' όλη τη διάρκεια της Παραγωγικής Λειτουργίας και Εγγύησης Καλής Λειτουργίας, και στην περίπτωση υπογραφής σύμβασης Συντήρησης, καθ' όλη τη διάρκεια της περιόδου Συντήρησης.

2.2. ΜΕΘΟΔΟΛΟΓΙΑ ΥΛΟΠΟΙΗΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΕΡΓΟΥ

Ο Ανάδοχος:

- ✓ Έχοντας διαμορφώσει μια σαφή και ολοκληρωμένη αντίληψη για το έργο,
- ✓ Λαμβάνοντας υπόψη την εμπειρία του και τις βέλτιστες διεθνείς πρακτικές που απορρέουν από την υλοποίηση παρόμοιων έργων, και
- ✓ Αξιολογώντας και κάνοντας χρήση των εργαλείων και μεθοδολογιών που αυτός διαθέτει,

υποχρεούται να παρουσιάσει στην Τεχνική Προσφορά του μια ολοκληρωμένη μεθοδολογική προσέγγιση που θα ακολουθήσει για την υλοποίηση του έργου.

2.2.1 Χρονοδιάγραμμα υλοποίησης Έργου

Η διάρκεια του έργου δεν πρέπει να ξεπερνά τους **2 μήνες (από την ημερομηνία αποδοχής του έργου)**.

Στην προσφορά τους οι υποψήφιοι Ανάδοχοι θα πρέπει να παραθέσουν αναλυτικό χρονοδιάγραμμα εργασιών, συμβατό με τη μεθοδολογία υλοποίησης και διαχείρισης έργου που θα ακολουθηθεί.

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα 1 - Πίνακας συστήματος ΣΥΛΛΟΓΗΣ, ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΑΡΧΕΙΩΝ ΚΑΤΑΓΡΑΦΗΣ (Security Information and Event Management)

Α/Α	ΠΡΟΔΙΑΓΡΑΦΗ	ΑΠΑΙΤΗΣΗ	ΑΠΑΝΤΗΣΗ	ΠΑΡΑΠΟΜΠΗ ΤΕΚΜΗΡΙΩΣΗΣ
	ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ			
1.	Αριθμός μονάδων	1		
2.	Να αναφερθεί μοντέλο και εταιρεία κατασκευής	ΝΑΙ		
	ΑΠΟΔΟΣΗ			
3	Ρυθμαπόδοση (ροές ανά δευτερόλεπτο)	>=1000 eps (event per second)		
	ΑΡΧΙΤΕΚΤΟΝΙΚΗ			
3.	Η προσφερόμενη λύση θα πρέπει να προσφέρεται υπό τη μορφή SW appliance, με όλο το απαραίτητο λογισμικό πλήρους εγκατεστημένου και παραμετροποιημένου από το Εργοστάσιο Κατασκευής.	ΝΑΙ		
4.	Η προσφερόμενη λύση θα πρέπει να είναι ανεξάρτητη από συστήματα Λογισμικού, να προσφέρεται υπό την μορφή "όλα σε ένα " (appliance), δίχως ανάγκες διαχείρισης Βάσεων Δεδομένων και Εξυπηρετητών Εφαρμογών (Application Servers).	ΝΑΙ		
5.	Η προσφερόμενη λύση θα πρέπει να υλοποιηθεί σε περιβάλλον εικονικοποίσης (virtualization) VMWare ESX .	ΝΑΙ		
6.	Η προσφερόμενη λύση θα πρέπει να διαθέτει εξειδικευμένη database (όχι σχεσιακή βάση δεδομένων) για την αποθήκευση των πρωτογενών ροών	ΝΑΙ		
	ΤΕΧΝΙΚΑ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ			
7.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει εγγενώς, δίχως ανάγκη ολοκλήρωσης τρίτων λύσεων, ανάλυση δικτυακής κίνησης σε πραγματικό χρόνο σε επίπεδο εφαρμογών Layer 7 (QFlows). Να προσφερθεί η αντίστοιχη αδειοδότηση	ΝΑΙ		
8.	Η προσφερόμενη λύση θα πρέπει να υποστηρίζει εγγενώς, δίχως ανάγκη ολοκλήρωσης τρίτων λύσεων, ανάλυση δικτυακής κίνησης σε πραγματικό χρόνο και εντοπισμού μη φυσιολογικής δικτυακής κίνησης (Network Anomaly Detection), τόσο φυσικού δικτύου (Netflow, JFlow, SFlow and cflowd) όσο και δικτύου εικονικών περιβαλλόντων VMWare ESX (Vflows). Να προσφερθεί η αντίστοιχη αδειοδότηση.	ΝΑΙ		
9.	Η προσφερόμενη λύση δεν πρέπει να βασίζει τον εντοπισμού κακόβουλων ενεργειών σε μηχανισμό υπογραφών	ΝΑΙ		

	(signatures), αλλά σε εγγενείς μηχανισμούς behavior profiling δικτυακής κίνησης περιλαμβανομένων πρωτοκόλλων επικοινωνίας / εφαρμογών / δικτύου. Να προσφερθεί η αντίστοιχη αδειοδότηση.			
10.	Να παρέχεται δυνατότητα επέκτασης λειτουργικότητας Risk Management από τον ίδιο Κατασκευαστή Λογισμικού	ΝΑΙ		
11.	Να παρέχεται δυνατότητα επέκτασης λειτουργικότητας DataBase Audit Monitoring από τον ίδιο Κατασκευαστή Λογισμικού, με εγγενείς δυνατότητες data base session analysis: SQL Analysis, real time alerts, correlation alerts, sensitive object classification	ΝΑΙ		
12.	Να παρέχεται δυνατότητα επέκτασης λειτουργικότητας DataBase Security από τον ίδιο Κατασκευαστή Λογισμικού, με εγγενείς δυνατότητες σε πραγματικό χρόνο: data base session blocking, termination, quarantine kai αλλοίωσης δεδομένων (data masking)	ΝΑΙ		
13.	Να υποστηρίζεται η διαχείριση των γεγονότων του δικτύου και της ασφάλειας	ΝΑΙ		
14.	Να υποστηρίζεται αυτοματοποιημένα η παραμετροποίηση των διαχειριζόμενων συσκευών	ΝΑΙ		
15.	Να υποστηρίζονται οι ακόλουθες συσκευές δικτύου και ασφαλείας: • Cisco Catalyst 6500 • Cisco ASA firewall • Checkpoint UTMs • Cisco Catalyst switches • Cisco Routers	ΝΑΙ		
16.	Να υποστηρίζονται τα ακόλουθα λειτουργικά συστήματα: • Windows Servers • Linux	ΝΑΙ		

	• AIX			
	ΑΠΟΤΙΜΗΣΗ ΕΥΠΑΘΕΙΩΝ			
17.	Η προτεινόμενη λύση να συνεργάζεται με εργαλεία αποτίμησης ευπαθειών όπως NMAP, Nessus, IBM App Scanner κ.λπ.	ΝΑΙ		
	ΔΙΑΧΕΙΡΙΣΗ			
18.	Το προσφερόμενο σύστημα να διαθέτει web γραφικό εργαλείο διαχείρισης	ΝΑΙ		
19.	Η αυθεντικοποίηση των διαχειριστών να γίνεται κατ' ελάχιστο με χρήση λογαριασμού και συνθηματικού	ΝΑΙ		
20.	Να υποστηρίζεται η δυνατότητα δημιουργίας ρόλων	ΝΑΙ		
21.	Η επικοινωνία των σταθμών εργασίας των διαχειριστών με το σύστημα να υλοποιείται με μηχανισμούς κρυπτογράφησης μέσω του πρωτοκόλλου SSL	ΝΑΙ		
	ΑΝΑΦΟΡΕΣ			
22.	Να παρέχονται έτοιμες προς χρήση αναφορές	ΝΑΙ		
23.	Να παρέχεται η δυνατότητα δημιουργίας custom αναφορών	ΝΑΙ		
24.	Να υποστηρίζονται αναφορές σε κανονιστικά πρότυπα	ΝΑΙ		
	ΑΣΦΑΛΕΙΑ ΣΧΕΣΙΑΚΩΝ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ			
25.	Να παρέχεται δυνατότητα DataBase Security από τον ίδιο Κατασκευαστή Λογισμικού, με εγγενείς δυνατότητες σε πραγματικό χρόνο: data base session blocking, termination, quarantine και αλλοίωσης δεδομένων (data masking). Να προσφερθεί η αντίστοιχη αδειοδότηση	ΝΑΙ		
26.	Να υποστηρίζονται Microsoft SQL και Oracle	ΝΑΙ		