ΠΡΟΔΙΑΓΡΑΦΗ ΕΝΟΠΛΩΝ ΔΥΝΑΜΕΩΝ

ΠΕΔ-Α-00421 ΕΚΔΟΣΗ 1η

ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΛΟΓΙΣΜΙΚΟΥ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΓΙΑ ΤΗΝ ΔΗΜΙΟΥΡΓΙΑ

ΚΕΝΤΡΟΥ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΚΥΒΕΡΝΟΧΩΡΟΥ ΣΤΗΝ ΠΟΛΕΜΙΚΗ ΑΕΡΟΠΟΡΙΑ

HAF-CIRC (HELLENIC AIRFORCE COMPUTER INCIDENT RESPONSE CENTER)

22 ΣΕΠΤΕΜΒΡΙΟΥ 2017

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΥΠΟΥΡΓΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Table of Contents

1. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

Η παρούσα Προδιαγραφή Ενόπλων Δυνάμεων (ΠΕΔ) καθορίζει τις απαιτήσεις προμήθειας καινούργιου Εξοπλισμού και Λογισμικού Πληροφορικής (Δικτυακές Συσκευές Ασφαλείας - Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας – Σχετικές Βιβλιοθήκες) για κάλυψη αναγκών δημιουργίας Κέντρου Αντιμετώπισης Περιστατικών Ασφάλειας Κυβερνοχώρου στην Πολεμική Αεροπορία. HAF-CIRC (Hellenic Airforce Computer Incident Response Center)

2. ΣΚΟΠΟΣ

Ο σκοπός της εν λόγω προμήθειας καλύπτει τις ανάγκες του Αδιαβάθμητου δικτυακού περιβάλλοντος του ΓΕΑ και συγκεκριμένα αφορά την παράδοση, εγκατάσταση, αρχική παραμετροποίηση του σχετικού δικτυακού εξοπλισμού και του αντίστοιχου λογισμικού ασφαλείας καθώς και την εκπαίδευση όπως περιγράφεται παρακάτω:

2.1. Λογισμικό ή/και Συσκευές Διαχείρισης Περιστατικών Ασφαλείας στο **Αδιαβάθμητο Δίκτυο του ΓΕΑ. Παράρτημα «Α»**

2.2. **Εγκατάσταση/Παραμετροποίηση/Υποστήριξη** Λογισμικού ή και Συσκευών Διαχείρισης Περιστατικών Ασφαλείας στο Διαβαθμισμένο και Αδιαβάθμητο Δίκτυο του ΓΕΑ. **Παράρτημα «Β»**

2.3. **Εκπαίδευση** για τη λειτουργία και διαχείριση του Λογισμικού ή και των συσκευών Διαχείρισης Περιστατικών Ασφαλείας για το Διαβαθμισμένο και Αδιαβάθμητο Δίκτυο του ΓΕΑ. **Παράρτημα «Γ»**

3. ΣΧΕΤΙΚΑ ΕΓΓΡΑΦΑ

ΕΛΟΤ EN ISO 27001 «Information Technology - Security Techniques – Information Security Management Systems - Requirements».

ΕΛΟΤ EN ISO 9001 «Quality Management Systems»

Νόμος 4412/2016 (Δημόσιες Συμβάσεις)

4. ΤΑΞΙΝΟΜΗΣΗ

Ο εξοπλισμός πληροφορικής που περιγράφεται στην παρούσα Προδιαγραφή ανήκει στις κλάσεις 7010 "Διαμόρφωση Συστήματος ADPE", 7030 "Λογισμικό ADPE" κατά NATO ACodP-2/3, ενώ οι σχετικοί κωδικοί κατά CPV είναι:

72000000-5 - IT services: consulting, software development, Internet and support

72100000-6 - Hardware consultancy services

72200000-7 - Software programming and consultancy services

72300000-8 - Data services

72400000-4 - Internet services

72500000-0 - Computer-related services

72510000-3 - Computer-related management services

72540000-2 - Computer upgrade services

72590000-7 - Computer-related professional services

72600000-6 - Computer support and consultancy services

72700000-7 - Computer network services

72800000-8 - Computer audit and testing services

72900000-9 - Computer back-up and catalogue conversion services

5. ΤΕΧΝΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

5.1. **Ορισμός Υλικού**

5.1.1. Ο υπό προμήθεια εξοπλισμός αποτελείται από το υλικό και το συνοδευτικό λογισμικό και περιλαμβάνει τα τεχνικά και λειτουργικά χαρακτηριστικά στοιχεία του Παραρτήματος «Α» αναλόγως της προτεινόμενης λύσης.

5.1.2. Όπου επιλεγεί η προμήθεια υλικού πρέπει να είναι καινούργια (δεν είναι αποδεκτά τα ανακατασκευασμένα υλικά).

5.1.3. Να μην υπάρχει ανακοίνωση περί αντικατάστασης των υπό προμήθεια υλικών.

5.1.4. Η προσφορά θα πρέπει να αναφέρεται σε πλήρες σύστημα (Υλικά - Λογισμικό – Υπηρεσίες από τον ίδιο προμηθευτή).

5.2. **Χαρακτηριστικά Επιδόσεων**

Όπως στο Παράρτημα «Α».

5.3. **Σχεδίαση και Κατασκευή**

Όλες οι επιμέρους συσκευές θα πρέπει να λειτουργούν με τροφοδοσία AC, 230V ± 10%, 50 Hz ± 0,5Hz. Το κριτήριο αυτό δεν ισχύει για την περίπτωση που θα επιλεγούν virtual appliances (VA).

5.4. **Εγκατάσταση**

Ο Ανάδοχος θα πρέπει να μεριμνήσει για την εγκατάσταση και πλήρη λειτουργία του συνόλου των ζητούμενων Συσκευών/Λογισμικού σε χώρο που θα υποδείξει η ΠΑ εντός διαστήματος 2 μηνών από την υπογραφή της σύμβασης ανάληψης έργου. Σύμφωνα με τα στοιχεία του Παραρτήματος «Β».

5.5. **Επισήμανση**

5.5.1. Σε κατάλληλη θέση επί όλων των συσκευών να επικολλάται, με μέριμνα του προμηθευτή, πινακίδα στην οποία να αναγράφονται τα εξής:

- Η ονομασία του υλικού.
- Ο αριθμός σύμβασης και έτος.
- Τα στοιχεία του Προμηθευτή (διεύθυνση, τηλέφωνο επικοινωνίας, e-mail).
- Ακριβής χρόνος λήξης εγγύησης-υποστήριξης.

6. ΕΓΓΥΗΣΗ - ΥΠΟΣΤΗΡΙΞΗ

6.1. **Χρόνος καλής λειτουργίας**

Ο προμηθευτής υποχρεούται να παρέχει εγγύηση-υποστήριξη καλής λειτουργίας τουλάχιστον τριών (3) ετών για τον εξοπλισμό-υλικά, η οποία αρχίζει μετά την οριστική παραλαβή τους. Σε κάθε περίπτωση υπερισχύει η περίοδος εγγύησης που αναγράφεται εντός του Παραρτήματος παρούσης ΠΕΔ, που περιγράφει το αντίστοιχο είδος του υλικού. Αν κατά την διάρκεια αυτού του χρονικού διαστήματος παρατηρηθεί βλάβη και ανωμαλία λειτουργίας η οποία οφείλεται σε ελαττωματικό υλικό ή εσφαλμένη εγκατάσταση, ο προμηθευτής υποχρεούται να την αποκαταστήσει με δική του δαπάνη (θα επισκευάζεται επί τόπου ή το υλικό θα παραλαμβάνεται προς επισκευή με έξοδα και μέριμνα του προμηθευτή).

6.2. **Οι υποχρεώσεις του Αναδόχου στο πλαίσιο εγγύησης καλής λειτουργίας, είναι:**

6.2.1. Αποκατάσταση των βλαβών και ανωμαλιών λειτουργίας του εξοπλισμού.

6.2.2. Αντικατάσταση των μέσων αποθηκεύσεως που παρουσιάζουν βλάβη κατά τη διάρκεια της εγγύησης.

6.2.3. Ανανεώσεις λογισμικού, βιβλιογραφίας, critical patch updates, software bugs και security fixes προκειμένου να εξασφαλισθεί η βέλτιστη λειτουργία των παρεχόμενων συστημάτων.

6.2.4. Παροχή support status και “End of Support/Life” ανακοινώσεις τουλάχιστον έξι (6) μήνες πριν την αλλαγή ενημέρωσης προϊόντος.

6.3. **Χρόνος απόκρισης - αποκατάστασης βλάβης - αντιμετώπισης περιστατικών ασφαλείας.**

6.3.1. Παροχή υποστήριξης μέσω email, web και phone Helpdesk (τουλάχιστον για τις καθημερινές ημέρες ωράριο 08:00-17:00), με δυνατότητα παραπομπής σύνθετων προβλημάτων για επί τόπου (on site) παρουσία ειδικών/τεχνικών στους χώρους που είναι εγκατεστημένο το υλικό. Δεδομένης της κρισιμότητας της υποδομής η ανταπόκριση (παρουσία) του αναδόχου σε περίπτωση βλάβης/δυσλειτουργίας ή αντιμετώπισης περιστατικού ασφαλείας θα πρέπει να είναι εντός εικοσιτεσσάρων (24) ωρών από τη στιγμή αναγγελίας ή/και επιβεβαίωσης της βλάβης. Εφόσον δεν αποκατασταθεί η λειτουργία του υλικού στο παραπάνω χρονικό διάστημα, ο Ανάδοχος θα πρέπει να μεριμνήσει για την αντικατάσταση του εντός των επόμενων 24 ωρών.

6.3.2. Η διάρκεια της περιόδου υποστήριξης θα είναι τρία (3) έτη από την υπογραφή της σύμβασης με δυνατότητα επέκτασης άλλων τριών (3) ετών. Στην υποστήριξη περιλαμβάνεται οποιουδήποτε είδους subscription χρειάζονται τα επιμέρους υποσυστήματα για να έχουν ανανεωμένες υπογραφές (signatures and hashes) καθώς και πρόσβαση σε βιβλιοθήκες ή άλλες βάσεις δεδομένων ανάλογα με το εξάρτημα/λογισμικό.

6.3.3. Το κόστος υποστήριξης για τρία (3) έτη περιλαμβάνεται στον προϋπολογισμό του έργου. Οι υποψήφιοι Ανάδοχοι θα πρέπει να συμπεριλάβουν στην οικονομική προσφορά το κόστος αυτό.

7. ΑΠΑΙΤΗΣΕΙΣ ΣΥΜΜΟΡΦΩΣΗΣ ΥΛΙΚΟΥ

7.1. **Συνοδευτικά Έγγραφα/Πιστοποιητικά**

7.1.1. Πιστοποίηση της κατασκευάστριας ή προμηθεύτριας εταιρείας κατά ISO 27001 «Information Technology - Security Techniques – Information Security Management Systems - Requirements» ή και κατά ISO 9001 «Quality Management System»

7.1.2. Ο εξοπλισμός να συνοδεύεται με κατάλληλα αποδεικτικά στοιχεία πιστοποιητικά, καταχωρήσεις στα εγχειρίδια υλικού κ.λ.π. τα οποία να είναι ευανάγνωστα, χωρίς διορθώσεις και να προκύπτει ότι αναφέρονται στο υπόψη υλικό.

8. ΛΟΙΠΕΣ ΑΠΑΙΤΗΣΕΙΣ

Απαράβατοι Όροι

Οι όροι της τεχνικής προδιαγραφής (κορμός και ανάλογα παραρτήματα), είναι απαράβατοι εκτός από τις περιπτώσεις που ρητώς αναφέρεται ότι πρόκειται για επιθυμητό κριτήριο. Η μη συμμόρφωση με τα βασικά κριτήρια συνεπάγεται και την απόρριψη της προσφοράς.

9. ΠΕΡΙΕΧΟΜΕΝΟ ΠΡΟΣΦΟΡΑΣ

Υποχρεώσεις Προμηθευτή

9.1. Υποβολή εγγράφων για αξιολόγηση

Όπως στα αντίστοιχα Παραρτήματα και επιπλέον να περιλαμβάνεται πίνακας συνθέσεως των προσφερόμενων υλικών στην οικονομική και στην τεχνική προσφορά χωρίς τιμές των επιμέρους υλικών.

9.2. Παράδοση Εγγράφων - Εντύπων – υλικών κατά την Παραλαβή

Τα προς προμήθεια υλικά να συνοδεύονται κατά την παραλαβή από πλήρη εγχειρίδια του χρήστη στα ελληνικά ή στα αγγλικά, σε έντυπη ή ηλεκτρονική μορφή και το απαραίτητο λογισμικό λειτουργίας.

9.3. Υποβολή από τον προμηθευτή του Φύλλου Συμμόρφωσης

Η αξιολόγηση κάθε προσφοράς θα γίνει με βάση το Φύλλο Συμμόρφωσης (ΦΣΜ). Ο κάθε προμηθευτής υποχρεούται να υποβάλλει ιδιαίτερο ΦΣΜ για την προσφορά του (όλες οι στήλες είναι υποχρεωτικές). Στο Φύλλο Συμμόρφωσης να αναφέρεται η αποδοχή κάθε όρου με παραπομπή στα σχετικά με τον όρο παραστατικά έγγραφα, όπου απαιτείται.

9.4. Υπόδειγμα Φύλλου Συμμόρφωσης όπως στο Παράρτημα «Δ».

10. ΣΗΜΕΙΩΣΕΙΣ

10.1. **Αξιολόγηση**

Η αξιολόγηση θα γίνει σύμφωνα με την εντολή προμήθειας. Οι παρατιθέμενοι όροι στον κορμό και στους πίνακες των Παραρτημάτων «Α», «Β», «Γ» και «Δ», έχουν την έννοια του διαχωρισμού της απαίτησης κατά στοιχεία προκειμένου να καταγραφεί η προσφορά του προμηθευτή με τη μορφή του φύλλου συμμόρφωσης και παρουσιάζουν την ελάχιστη απαίτηση της Υπηρεσίας.

10.2. **Παραπομπές.**

Όπου γίνεται παραπομπή σε πρότυπα, αναφορά σε πιστοποιητικά, σήματα, διπλώματα ευρεσιτεχνίας ή τύπους, ή αναφορά σε ορισμένη παραγωγή ή προέλευση κ.λ.π. κατά τις διατάξεις των άρθρων 54, 55 και 56 του ν. 4412/2016 νοούνται και τα «ισοδύναμα».

11. ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ «Α» στην ΠΕΔ-Α-00421/22 ΣΕΠ 17

ΠΙΝΑΚΑΣ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΛΟΓΙΣΜΙΚΟΥ / ΣΥΣΚΕΥΩΝ ΑΣΦΑΛΕΙΑΣ

Αδιαβάθμητο Δίκτυο του ΓΕΑ

Α/Α	Περιγραφή/Κριτήριο
1.	**Το παρόν προϊόν αποτελεί <u>υποχρεωτική</u> απαίτηση**. Το προϊόν τύπου Security Information and Event Management - **SIEM** (physical ή Virtual) να μπορεί να συλλέξει, αποθηκεύσει και επεξεργαστεί καταγραφές (logs) σε πραγματικό χρόνο από διαφορετικές δικτυακές υπηρεσίες, εξυπηρετητές και συσκευές (πχ. Routers, Firewalls, IDS/IPS) που αποτελούν τμήμα του αδιαβάθμητου στρατιωτικού δικτύου της ΠΑ προκειμένου να επιτευχθούν τα εξής: • Δυνατότητα ενσωμάτωσης καταγραφών από τουλάχιστον 130 διαφορετικές δικτυακές συσκευές ή διευθύνσεις (IP). • Αυτόματη συλλογή, κανονικοποίηση, κατηγοριοποίηση και ασφαλή αποθήκευση καταγραφών με δυνατότητα αποθήκευσης στοιχείων του τελευταίου 1 μήνα. (Log collection, normalization and secure retention) • Δυνατότητα αποθήκευσης πλήθος καταγραφών ≥ $150x10^6$ Events (για την περίπτωση physical appliance) • Αναζήτηση και ανάλυση καταγραφών (Event/Log Search/Analysis) • Παρακολούθηση και συσχετισμό απειλών σε πραγματικό χρόνο με ρυθμό μεγαλύτερο από ≥ 800 EPS (Events per Second). (Real-time Monitoring & Correlation of threats) • IDS throughput > 80Mbps • Δημιουργία αναφορών ασφαλείας, απειλών και συμμόρφωσης κατά ISO 27001. Υποστήριξη PCI DSS, HIPAA και επιπλέον προτύπων θα αξιολογηθεί θετικά. (Security, Threat and Compliance Reporting) • Δυνατότητα παραγωγής καταγραφών και διαχείρισης περιστατικών ασφαλείας με ρυθμό μεγαλύτερο από ≥ 800 EPS (Events per Second). • <u>Log Analysis</u> / Η προτεινόμενη λύση πρέπει να: – Διαθέτει δυνατότητα συσχετισμού των συλλεγόμενων logs για περιστατικά ασφαλείας, στηριζόμενη σε out of the box κανόνες προκειμένου να αναγνωρίζει γνωστές απειλές και περιστατικά ασφαλείας. – Υποστηρίζει την δημιουργία κανόνων συσχετισμού (correlation rules) για συλλεγόμενα logs με εύχρηστο και γρήγορο τρόπο. – Εκτελεί anomaly detection, βασιζόμενη σε προκαθορισμένες συμπεριφορές (preconfigured behavior) ανά σύστημα ασφαλείας προκειμένου να αναγνωρίζει ύποπτα περιστατικά/συμπεριφορές και να δημιουργεί αντίστοιχες προειδοποιήσεις (alerts). – Συσχετίζει logs από διαφορετικές πηγές ειδοποιώντας τον χρήστη για περιστατικά ασφαλείας σε real ή near-real time. – Υποστηρίζει δυνατότητα κρισιμότητας των συστημάτων την οποία και λαμβάνει υπόψη στον χαρακτηρισμό των περιστατικών. • <u>Administration – Operation</u> / Η προτεινόμενη λύση πρέπει να: – Παρέχει στον χρήστη την δυνατότητα προσαρμογής του γραφικού περιβάλλοντος (πχ αλλαγή στηλών, απόκρυψη περιστατικών ή logs). Επίσης να δίνει την δυνατότητα στον χρήστη να επιλέγει logs από

	δύο ή περισσότερες πηγές ταυτόχρονα. – Παρέχει γρήγορη εύρεση των περιστατικών με δυνατότητα επιλογής κριτηρίων από τον χρήστη. – Δυνατότητα πρόσβασης στους χρήστες με διαφορετικούς ρόλους ανάλογα με τις ανάγκες της ΠΑ. (**επιθυμητό**) – Δυνατότητα να συμπεριλάβει out-of-the-box / αναφορές και προειδοποιήσεις σύμφωνα με τις ανάγκες συμμόρφωσης ανάλογα με την εθνική νομοθεσία, τα διεθνή πρότυπα και την βέλτιστη πρακτική (best practice). (**επιθυμητό**) – Υποστηρίζει την δημιουργία προσαρμοσμένων στις απαιτήσεις του χρήστη αναφορών, με δυνατότητα αποθήκευσης αυτών για μελλοντική χρήση, με φιλικό προς τον χρήστη και γρήγορο τρόπο. • Solution Architecture / Η προτεινόμενη λύση πρέπει να: – Διαθέτει δυνατότητα συνεργασίας με φυσικές ή εικονικές συσκευές – Διαθέτει δυνατότητα σύνδεσης σε standard rack (σε περίπτωση physical device). – Διαθέτει δυνατότητα επεκτασιμότητας προκειμένου να μπορεί να διαχειριστεί μεγαλύτερο όγκο δεδομένων/καταγραφών λόγω αύξησης των συσκευών ή λόγω επέκτασης της περιόδου χρήσης. – Διαθέτει δυνατότητα κρυπτογραφημένης πρόσβασης στο γραφικό περιβάλλον της εφαρμογής, κρυπτογράφησης των δεδομένων, ενσωμάτωσης active Directory, access control για τον χρήστη, NTP Client και SNMP. (**επιθυμητό**) • Threat Intelligence / Η προτεινόμενη λύση πρέπει να: – Διαθέτει δυνατότητα threat intelligence ώστε να χρησιμοποιηθούν για εργασίες advanced analytics προκειμένου να αναγνωρίζονται γνωστές και άγνωστες απειλές σύμφωνα με το σύγχρονο περιβάλλον απειλών. • Report/Alert Generation / Η προτεινόμενη λύση πρέπει να: – Διαθέτει δυνατότητα αυτόματων/προγραμματισμένων και προσαρμοσμένων αναφορών ανάλογα με τις απαιτήσεις της ΠΑ. – Μπορεί να αναλύσει σε λεπτομέρεια τις αναφορές προκειμένου να εξαχθούν συμπεράσματα των περιστατικών ασφαλείας. – Διαθέτει δυνατότητα εξαγωγής δεδομένων/αναφορών σε μορφή PDF, XLS και CSV. (**επιθυμητό**) – Δημιουργεί διάφορους τύπους προειδοποιήσεων με αυτοματοποιημένο τρόπο αλλά και με κανόνες. – Μπορεί να στείλει προειδοποιήσεις μέσω email ανάλογα με την κρισιμότητα των περιστατικών ασφαλείας. (**επιθυμητό**)
2.	**Το προϊόν είναι υποχρεωτικό και δύναται να αποτελεί μέρος του SIEM (προϊόν 1 παρόντος Παραρτήματος**). Λογισμικό με δυνατότητα εύρεσης αδυναμιών των δικτυακών συσκευών (**Vulnerability scanner**) με τα εξής χαρακτηριστικά. • Δυνατότητα εντοπισμού και ελέγχου (asset discovery and scanning) όλων των δικτυακών συσκευών με αυτοματοποιημένο τρόπο. • Δυνατότητα επιλογής της περιοδικότητας και έντασης του ελέγχου. (**επιθυμητό**) • Δυνατότητα δημιουργίας αυτοματοποιημένης αναφοράς ιεραρχημένης ανάλογα με την σοβαρότητα των ευρημάτων και το επίπεδο του ρίσκου. • Δυνατότητα συσχέτισης τρωτοτήτων με αριθμούς CVE (Common Vulnerability and Exposure). (**επιθυμητό**) • Δυνατότητα γραφικής παρουσίασης των αποτελεσμάτων. (**επιθυμητό**) • Το προϊόν θα πρέπει να ελαχιστοποιεί περιστατικά δυσλειτουργίας των τερματικών λόγω της δραστηριότητάς του. • Θα πρέπει να παρέχει εύκολη δυνατότητα προσαρμογής της λειτουργίας

	του σε συγκεκριμένο αριθμό τερματικών. (**επιθυμητό**) • Υποστήριξη πλήθους πρωτοκόλλων και Λειτουργικών Συστημάτων (Windows, Linux, MAC)
3.	**Το παρόν προϊόν είναι επιθυμητό μόνο στην περίπτωση που έχει εξασφαλιστεί η προμήθεια το προϊόντων 1 και 2 παρόντος Παραρτήματος.** Λογισμικό (physical ή Virtual Appliance) ή/και συσκευή προστασίας των Διαδικτυακών εφαρμογών (**Web Application Firewall**) το οποίο να είναι σε θέση να: • Ανιχνεύσει και σταματήσει γνωστές και άγνωστες (zero day attacks) επιθέσεις εναντίον των υποστηριζόμενων δικτυακών εφαρμογών που παρέχονται μέσω της ιστοσελίδας της ΠΑ αλλά και της σχετικής δικτυακής υποδομής που την υποστηρίζει (Servers). • Προστατεύσει από διαδικτυακές επιθέσεις/απειλές όπως περιγράφονται στο WASC Web Security Attack classification. (**επιθυμητό**) • Προστατεύσει από διαδικτυακές επιθέσεις/απειλές όπως περιγράφονται από τον OWASP Top Ten vulnerabilities. • Καθώς και από τις εξής επιθέσεις Web: SQL injection, OS command injection, LDAP injection, SSI injections, XPath injection, Sensitive information leakage (e.g. CCN, SSN, custom defined), Application DOS, CSRF, parameter tampering, Form field manipulation, Session hijacking, Cookie poisoning, Application buffer overflow, Brute force, Access to predictable resource locations, Unauthorized navigation, Web server reconnaissance, Directory\path traversal, Forceful browsing, HotLink, HTTP response splitting, Evasion and illegal encoding, XML validation, Web services method restrictions and validation, HTTP RFC violations, HTTP request format and limitation violations (size, unknown method, etc.), Use of revoked or expired client certificate, File upload violations. (**επιθυμητό**) • Υποστηρίξει εφαρμογή πολιτικών ανεξάρτητα από την κωδικοποίηση χαρακτήρων προκειμένου να προστατεύσει από επιθέσεις που χρησιμοποιούν τεχνικές αποφυγής όπως: URL-decoding (for example %XX), Self-referencing paths (that is,. use of /./ and encoded equivalents), Path back-references (that is, use of /../ and encoded equivalents), Mixed case, Excessive use of whitespace, Comment removal (for example, convert DELETE/**/FROM to DELETE FROM), Conversion of (Windows-supported) backslash characters into forward slash characters, Conversion of IIS-specific Unicode encoding (%uXXYY), IIS extended Unicode, Virtual directory route—positive folder enforcement, Base64 Encoding. (**επιθυμητό**) • Υποστηρίξει την εφαρμογή μοτίβων ροής εντός της εφαρμογής που προστατεύεται έτσι ώστε να εξασφαλίζεται ότι η ροή επίσκεψης του χρήστη εντός της εφαρμογής είναι συνεπής με την αναμενόμενη συμπεριφορά. (**επιθυμητό**) • Συσχετίσει (correlate) τις καταγραφές του με αυτές του SIEM αλλά και άλλων δικτυακών συσκευών ασφαλείας. (**επιθυμητό**) • Λειτουργήσει χρησιμοποιώντας positive security model με δυνατότητας εκμάθησης και ορισμού των κανόνων που περιγράφουν την αναμενόμενη συμπεριφορά μίας εφαρμογής ή υπηρεσίας και τερματισμού της κίνησης που δεν συμμορφώνεται με αυτούς τους κανόνες. (**επιθυμητό**) • Λειτουργήσει ως reverse proxy προστατεύοντας από επιθέσεις μέσω της δημιουργίας νέων κατάλληλα διαμορφωμένων αιτημάτων ή μέσω απόρριψής τους. (**επιθυμητό**) • Έχει τη δυνατότητα λειτουργίας και ως out-of-path monitor και ως transparent bridge. (**επιθυμητό**) • Έχει τη δυνατότητα εμφάνισης στο χρήστη παραμετροποιήσιμου μηνύματος σφάλματος σε περίπτωση απόρριψης αιτήματος. (**επιθυμητό**)

	• Έχει τη δυνατότητα επιθεώρησης και απόρριψης ανεπιθύμητων/ κακόβουλων/ άκυρων HTTP/SOAP/XML/JSON αιτημάτων. (**επιθυμητό**) • Υποστηρίζει allow list, brute-force, database, files upload, global parameters, http methods, logging, parameters, path-blocking, safe-reply, session, vulnerabilities, Web Services, XML φίλτρα ασφαλείας. (**επιθυμητό**) • Υποστηρίζει την αναγνώριση trusted hosts έτσι ώστε η συσκευή να μπορεί να μαθαίνει μόνο νόμιμη κίνηση. (**επιθυμητό**) • Υποστηρίζει highly granular policy control βασισμένο στο μονοπάτι της εφαρμογής, εκμάθηση εφαρμογής χωρίς manual μεσολάβηση, επιθεώρηση της εγκατεστημένης και ενεργής πολιτικής στη συσκευή, αυτόματη αναβάθμιση επιπέδου προστασίας με βάση τον εντοπισμό επίθεσης, εντοπισμό αλλαγών διαμόρφωσης, αυτόματες αλλαγές ρυθμίσεων στα φίλτρα ασφαλείας βάση της κίνησης και στατιστικών δεδομένων. (**επιθυμητό**) • Παρέχει γραφικό περιβάλλον διεπαφής (GUI) με τη δυνατότητα διαμόρφωσης διαφορετικών πολιτικών για κάθε υποστηριζόμενη εφαρμογή. Το GUI να είναι ασφαλές και αξιόπιστο και να μην είναι ευάλωτο σε καμία από τις επιθέσεις από όσες το σύστημα έχει σχεδιαστεί να παρέχει προστασία. • Παρέχει απλές κοινές λειτουργίες διαχείρισης όπως ενημέρωση πολιτικών ασφαλείας και ρύθμισή τους για τη μείωση των false positives καθώς και δυνατότητα manual αποδοχής ενός false positive με απλό τρόπο. (**επιθυμητό**) • Υποστηρίζει out-of-the-box πολιτικές ασφαλείας βασισμένες στο negative security model αντιμετωπίζοντας μεγάλο εύρος απειλών. • Παρέχει δυνατότητα παραμετροποίησης πολιτικών άρνησης υπηρεσιών (denial of service). (**επιθυμητό**) • Υποστηρίζει τη δυνατότητα ορισμού trusted hosts που θα έχουν τη δυνατότητα να εκτελέσουν λειτουργίες που απαγορεύονται από την ενεργή πολιτική ασφαλείας όπως penetration testing ή troubleshooting. • Υποστηρίζει δυνατότητα παρακολούθησης της απόδοσης και της λειτουργίας της συσκευής με χρήση των πρωτοκόλλων SNMP και syslog και αποστολή ειδοποιήσεων (alerts) μέσω email. (**επιθυμητό**) • Υποστηρίζει την παραγωγή στατιστικών απόδοσης του συστήματος, αναφορών περιστατικών των εφαρμογών και των φίλτρων ασφαλείας, αυτόματη και κατά απαίτηση παραγωγή αναφορών σε human-readable format καθώς και αυτόματη διανομή τους. • Υποστηρίζει δυνατότητα τριών (3) modes λειτουργίας: Bypass, Passive, Active. (**επιθυμητό**) • Υποστηρίζει ασφαλή απομακρυσμένη υπηρεσία διαχείρισης με Role Based Access Control. (**επιθυμητό**) • Υποστηρίζει την εξαγωγή και εισαγωγή κανόνων και πολιτικών ασφαλείας σε άλλο σύστημα. (**επιθυμητό**) • Παρέχει απλοποιημένο σύστημα διαχείρισης και ελέγχου με δυνατότητα κεντρικοποιημένου συγχρονισμού της διαμόρφωσης και των δεδομένων εκμάθησης σε όλες τις συσκευές. • Παρέχει RESTful API(**επιθυμητό**) • Παρέχει ενημερώσεις λογισμικού σε τακτικά διαστήματα. • Παρέχει προσωρινά code patches ή hot fixes μεταξύ των κανονικών εκδόσεων λογισμικού. (**επιθυμητό**) • Παρέχει λεπτομερή και ενημερωμένη βιβλιογραφία διαθέσιμη off-line.
4.	**Το παρόν προϊόν είναι επιθυμητό μόνο στην περίπτωση που έχει εξασφαλιστεί η προμήθεια το προϊόντων 1 και 2 παρόντος Παραρτήματος.** Λογισμικό (συμπεριλαμβάνονται Virtual Appliances) ή συσκευή τύπου **Email**

Filtering για την προστασία του διακομιστή ηλεκτρονικών μηνυμάτων (email server) με τα εξής χαρακτηριστικά:

- Να μπορεί να ανιχνεύσει εξετάσει τα εισερχόμενα email για την ύπαρξη κακόβουλων συνημμένων αρχείων.
- Να μπορεί να ανιχνεύσει/εξετάσει τα εισερχόμενα email για την ύπαρξη κακόβουλων συνδέσμων (Phishing URLs) σε HTTP και HTTPS.
- Διαθέτει δυνατότητα προστασίας από στοχευμένες επιθέσεις spear-phishing. (**επιθυμητό**)
- Διαθέτει δυνατότητα προστασίας email από γνωστές και άγνωστες επιθέσεις (**επιθυμητό**).
- Διαθέτει δυνατότητα τοποθέτησης των αναγνωρισμένων ιών σε ξεχωριστό φάκελο (quarantine folder) προσβάσιμο μόνο από τον διαχειριστή.
- Διαθέτει δυνατότητα φραγμού κακόβουλων emails.
- Διαθέτει δυνατότητα υποστήριξης, Message Transfer Agent(MTA), SPAN/TAP Deployment και BCC Deployment. (**επιθυμητό**)
- Διαθέτει δυνατότητα υποστήριξης πολύπλοκης αρχιτεκτονικής MTA με υποστήριξη TLS. (**επιθυμητό**)
- Διαθέτει δυνατότητα ενσωμάτωσης με Web και Endpoint security λύση. (**επιθυμητό**)
- Διαθέτει δυνατότητα anti-APT και όχι μόνο ως add-on. (**επιθυμητό**)
- Διαθέτει δυνατότητα dynamic inspection των συνδέσμων (links) στο σώμα των email χωρίς να επιτρέπει στον χρήστη να επιλέξει τον σύνδεσμο (without end-user click on).
- Διαθέτει δυνατότητα download και ανάλυσης των συνδέσμων που έχουν ως στόχο συγκεκριμένο φάκελο. (**επιθυμητό**)
- Διαθέτει δυνατότητα ελέγχου των attachments ακόμα και εάν προστατεύονται από κωδικό, χρησιμοποιώντας πιθανούς κωδικούς από το σώμα των email, από έτοιμες λίστες κωδικών και από ανανεώσεις του προμηθευτή. (**επιθυμητό**)
- Να υποστηρίζει την αποστολή κωδικών πρόσβασης που ορίζονται από τον πελάτη για αποκρυπτογράφηση συνημμένων που προστατεύονται με κωδικό πρόσβασης. (**επιθυμητό**)
- Οι εικονικές μηχανές που χρησιμοποιούνται για το άνοιγμα των αρχείων πρέπει να έχουν τη δυνατότητα να ανοίξουν το ίδιο συνημμένο με διαφορετικό λογισμικό (π.χ. αρχείο PDF να μπορεί να ανοιχτεί με διαφορετικές εκδόσεις λειτουργικών συστημάτων και διαφορετικές εκδόσεις του Acrobat Reader την ίδια στιγμή. (**επιθυμητό**)
- Η δυναμική εκτέλεση των φακέλων πρέπει να μπορεί να δημιουργήσει τους εξής ενδείκτες επίθεσης: (**επιθυμητό**)
  - Αλλαγές στη registry
  - Κλήσεις API
  - Δημιουργία, ανάγνωση και διαγραφή φακέλων
  - Αλλαγές στο λειτουργικό
  - Συνδέσεις δικτύου
  - Απαντήσεις DNS
- Δυνατότητα δυναμικής ανάλυσης που να υποστηρίζει μηχανισμούς MD5 και SHA1 hashing.
- Υποστηρίζει την εξαγωγή ενδεικτών επίθεσης από τη δυναμική ανάλυση και την χρήση τους σε άλλα δικτυακά συστήματα άμυνας προκειμένου να ελέγξει για παραβιάσεις.(**επιθυμητό**)
- Δυνατότητα προσθήκης κανόνων YARA για τον έλεγχο των email. (**επιθυμητό**)
- Δυνατότητα προειδοποιήσεων μέσω HTTP(s) SYSLOG, SMTP and SNMP(**επιθυμητό**)
- Δυνατότητα ελέγχου των εξής extensions: 3gp, applet, asf, avi, bat, chm,

	cmd, com, csv, dll, doc, docx, eeml, eml, exe, flv, gif, hlp, hml, htm, hwp, hwt, ico, jar, jpg, js, lnk, mht, midi, mov, mp3, mp4, mpg, msi, pdf, png, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav, wma, wsf, xdp, xls, xslx, xml. • Δυνατότητα θύρας Intelligence Platform Management Interface (IPMI). (**επιθυμητό**)
	Γενικά κριτήρια
5.	Κάθε προτεινόμενο προϊόν πρέπει να είναι καινούριο, να κυκλοφορεί στη διεθνή αγορά και να μην υπάρχει ανακοίνωση περί αντικατάστασης/απόσυρσής του.
6.	Να ακολουθεί διεθνή πρότυπα εξοπλισμού ηλεκτρολογικής ασφάλειας (CE), ηλεκτρομαγνητικής συμβατότητας (EMC), ηλεκτρομαγνητικών παρεμβολών (EMI), εξοικονόμησης ενέργειας (Energy Star) στην περίπτωση φυσικών μηχανημάτων**.** Το παρόν κριτήριο δεν ισχύει στην περίπτωση που προταθούν virtual appliances.
7.	Να διαθέτει υποστήριξη τριών (3) ετών τουλάχιστον.

ΠΑΡΑΡΤΗΜΑ «Β» στην ΠΕΔ-Α-00421/22 ΣΕΠ 17

ΕΓΚΑΤΑΣΤΑΣΗ/ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ/ΥΠΟΣΤΗΡΙΞΗ

ΛΟΓΙΣΜΙΚΟΥ Η/ΚΑΙ ΣΥΣΚΕΥΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

ΣΤΟ ΑΔΙΑΒΑΘΜΗΤΟ ΔΙΚΤΥΟ ΤΟΥ ΓΕΑ.

Α/Α	Κριτήριο – Υποχρεωτική Απαίτηση
1.	Ο προμηθευτής είναι υποχρεωμένος σε συνεργασία με προσωπικό της ΠΑ να: • Εγκαταστήσει, ρυθμίσει, παραμετροποιήσει όλα τα συστήματα των Παραρτημάτων Α και Β προκειμένου αυτά να είναι σε θέση να λειτουργήσουν σύμφωνα με τις προδιαγραφές τους και χωρίς να δημιουργούν προβλήματα στην δικτυακή υποδομή που θα εγκατασταθούν. • Προτείνει τις απαραίτητες αλλαγές σε ότι αφορά την υπάρχουσα υποδομή των δικτύων προκειμένου να επιτευχθεί η μέγιστη δυνατή ασφάλεια χωρίς να παρεμποδίζεται η λειτουργία των δικτυακών υπηρεσιών της ΠΑ. • Να προτείνει συγκεκριμένες διαδικασίες σε ότι αφορά τις πολιτικές διαχείρισης και αντιμετώπισης περιστατικών ασφαλείας. (**επιθυμητό**) • Να εκτελέσει τους απαραίτητους ελέγχους αποδοχής πριν την παράδοση των ανωτέρω υλοποιήσεων ασφαλείας. (**επιθυμητό**) • Όλα τα προσφερόμενα συστήματα θα γίνουν αποδεκτά μόνο εφόσον όλα τα απαραίτητα χαρακτηριστικά/λειτουργίες ελεγχθούν και γίνουν αποδεκτά με γραπτό τρόπο από την ΠΑ.
2.	Ο προμηθευτής είναι υποχρεωμένος να διαθέτει τα παρακάτω χαρακτηριστικά : • Δραστηριοποίηση στο χώρο της ασφάλειας Πληροφορικής τουλάχιστον τα τελευταία 5 έτη. • Cyber Security References (τουλάχιστον 3) με έργα ανάλογης πολυπλοκότητας, αντικειμένου και έκτασης. (**επιθυμητό**)

ΕΚΠΑΙΔΕΥΣΗ

ΓΙΑ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ Η/ΚΑΙ ΤΩΝ ΣΥΣΚΕΥΩΝ ΔΙΑΧΕΙΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΟ ΑΔΙΑΒΑΘΜΗΤΟ ΔΙΚΤΥΟ ΤΟΥ ΓΕΑ

Πρόγραμμα Εκπαίδευσης - Γενικά

Ο ανάδοχος είναι υποχρεωμένος να εκπαιδεύσει προσωπικό της ΠΑ το οποίο θα επανδρώσει το CIRC. Το εν λόγω προσωπικό θα επιλεγεί με ευθύνη της ΠΑ και θα διαθέτει ήδη γνώσεις Πληροφορικής στα εξής αντικείμενα: Πρωτόκολλα TCP/IP και OSI, λειτουργία βασικών δικτυακών συσκευών (routers, switches, κλπ.), λειτουργικά συστήματα Windows και Linux/Unix, διαχείριση Firewalls, δικτυακές εφαρμογές, Βάσεις Δεδομένων, γνώσεις προγραμματισμού (ενδεικτικά Bash scripting και κάποια από: Python, Java, C#, C++ κλπ), κατηγορίες επιθέσεων και ιομορφικού λογισμικού (Virus, Trojans, backdoor, malware) και εργασιακή εμπειρία σε θέση με αντικείμενα ασφάλειας Πληροφορικής.

Α/Α	Κριτήριο – Υποχρεωτική Απαίτηση
1.	Η εκπαίδευση του αναδόχου θα περιλαμβάνει τα παρακάτω αντικείμενα: – Παροχή γνώσεων σχετικά με τον τύπο και την μεθοδολογία των επιθέσεων σε δικτυακό περιβάλλον, τρόπους αναγνώρισης, ιεράρχησης και αντιμετώπισης των επιθέσεων. – Ανάλυση και εξάσκηση (Platform Specific) σε ότι αφορά την τεχνολογία, τις διαδικασίες ασφάλειας, τις ρυθμίσεις των δικτυακών εργαλείων και την παραμετροποίηση των μηχανών SIEM, WAF, Vulnerability Scanner, Mail Filtering που θα επιλεγούν. – Ασφάλεια καταγραφών (Log Files) και των αντίστοιχων βάσεων δεδομένων που δημιουργούνται από τα SIEM, WAF, Mail Filtering που θα επιλεγούν. – Επιλογή κατάλληλων στοιχείων και δημιουργία αναφορών περιστατικών ασφαλείας. – Δημιουργία πολιτικών διαχείρισης περιστατικών ασφαλείας. – Το πρόγραμμα πρέπει να καταλήγει σε γραπτή πιστοποίηση των εκπαιδευόμενων από την εταιρεία. – Το πρόγραμμα εκπαίδευσης πρέπει να υφίσταται στην αντίστοιχη βιομηχανία τουλάχιστον τα τελευταία 3 έτη. Περισσότερα έτη θα αξιολογηθούν θετικά. (**επιθυμητό**)

ΠΑΡΑΡΤΗΜΑ «Δ» στην ΠΕΔ-Α-00421/22 ΣΕΠ 17

ΥΠΟΔΕΙΓΜΑ ΠΙΝΑΚΑ ΦΥΛΛΟΥ ΣΥΜΜΟΡΦΩΣΕΩΣ

Α/Α παραγράφου Παραρτήματος	**ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ**		**Παραπομπή σε Τεχνικά, Εγχειρίδια, Prospectus**
	Κριτήριο – Υποχρεωτική Απαίτηση	**ΑΠΑΝΤΗΣΗ ΠΡΟΣΦΕΡΟΜΕΝΟΥ**	
(1)	(2)	(3)	(4)
1.	Αναγράφεται η αντίστοιχη παράγραφος του Παραρτήματος [π.χ για το Α1 (α/α 1 παρ. Α) Το προϊόν τύπου Security Information……)	Συμφωνώ	
2.		Συμφωνώ	
3.		Συμφωνώ	
4.		Συμφωνώ	
		Να αναφερθούν όλα τα τεχνικά λειτουργικά χαρακτηριστικά του προσφερόμενου υλικού κατά αντιστοιχία του πίνακα του αντίστοιχου παραρτήματος	

ΠΑΡΑΤΗΡΗΣΕΙΣ:

1. Ακολουθείται αυστηρά η σειρά των παραγράφων στα αντίστοιχα παραρτήματα.

2. Τα χαρακτηριστικά των συσκευών (εάν υπάρχουν) θα δίνονται σε μονάδες και περιγραφές σύμφωνα με τα αναγραφόμενα στην προδιαγραφή. Αν η διατύπωση είναι διαφορετική στα επίσημα PROSPECTUS, θα δοθούν οι τύποι μετατροπής.

3. Η συμπλήρωση όλων των παραγράφων της προδιαγραφής στις στήλες (3) και (4) είναι υποχρεωτική για τον προμηθευτή.

4. Αν τα χαρακτηριστικά του προσφερόμενου υλικού διαφέρουν από αυτά της προδιαγραφής θα πρέπει να επισυνάπτεται εξήγηση για το πως ικανοποιούνται οι απαιτήσεις της Υπηρεσίας από το προσφερόμενο σύστημα.

5. Πάνω στα prospectus των υλικών να σημαίνεται ιδιόχειρα κάθε σημείο παραπομπής, ούτως ώστε να μην αναγκάζεται η επιτροπή βαθμολογίας να αναζητά μέσα στο

κείμενο το συγκεκριμένο σημείο. Ιδιαίτερα θα εκτιμηθεί η χρήση δεικτών στις αντίστοιχες σελίδες παραπομπής για ταχεία ανεύρεσή τους.

6. Το ΦΣΜ πρέπει να συμφωνεί πλήρως με τα προσφερόμενα υλικά όπως φαίνονται στην οικονομική προσφορά και στους πίνακες συνθέσεως. Π.χ. δεν είναι δυνατόν στο ΦΣΜ να αναγράφεται ότι προσφέρεται βάση στήριξης (dock station) και στην οικονομική προσφορά αυτό να δίνεται σαν "OPTION" με επιπλέον χρέωση.

ΑΠΑΓΟΡΕΥΟΝΤΑΙ στο ΦΣΜ οι χειρόγραφες διορθώσεις και προσθήκες, καθώς και οι διαγραφές με διορθωτικό ή άλλο τρόπο.

	ΕΓΚΡΙΣΗ ΤΕΧΝΙΚΗΣ ΠΡΟΔΙΑΓΡΑΦΗΣ ΣΥΝΤΑΞΗ
	ΕΛΕΓΧΟΣ
	ΘΕΩΡΗΣΗ ΗΜΕΡΟΜΗΝΙΑ