ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗΣ ΑΝΑΠΤΥΞΗΣ (Ε.Κ.Ε.Τ.Α.) /
Ινστιτούτο Εφαρμοσμένων Βιοεπιστημών (ΙΝΕΒ)

Θεσσαλονίκη, 06-05-2021
Αριθμ. Πρωτ.: 001484

ΠΡΟΣΚΛΗΣΗ ΕΝΔΙΑΦΕΡΟΝΤΟΣ ΚΑΙ ΚΑΤΑΘΕΣΗΣ ΠΡΟΣΦΟΡΩΝ ΓΙΑ ΤΗΝ ΑΝΑΘΕΣΗ ΤΗΣ ΠΡΟΜΗΘΕΙΑΣ

«Προμήθεια Αδειών Λειτουργίας για Πακέτο Λογισμικού Ασφαλείας»

Το Εθνικό Κέντρο Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ) / Ινστιτούτο Εφαρμοσμένων Βιοεπιστημών (ΙΝΕΒ), νομικό πρόσωπο ιδιωτικού δικαίου, μη κερδοσκοπικού χαρακτήρα, που εδρεύει στη Θέρμη Θεσσαλονίκης, 6ο χλμ. Οδού Χαριλάου-Θέρμης, προσκαλεί κάθε ενδιαφερόμενο (φυσικό ή νομικό πρόσωπο, ή ενώσεις και κοινοπραξίες αυτών) να υποβάλει πρόταση – προσφορά, μη δεσμευτική για το ΕΚΕΤΑ, σύμφωνα με τις τεχνικές προδιαγραφές της παρούσας πρόσκλησης, για την ανάθεση της προμήθειας :

«Προμήθεια Αδειών Λειτουργίας για Πακέτο Λογισμικού Ασφαλείας»

Η συνολική δαπάνη της προμήθειας δεν πρέπει να υπερβαίνει τις **επτά χιλιάδες επτακόσια ένα ευρώ και εξήντα δύο λεπτά (7.701,62 €) μη συμπεριλαμβανομένου του ΦΠΑ**.

Οι υποψήφιοι θα πρέπει να έχουν αποδεδειγμένη επαγγελματική εμπειρία στην υλοποίηση αντίστοιχων προμηθειών και η προσφορά τους να πληροί τις Τεχνικές Προδιαγραφές της παρούσας Πρόσκλησης.

Οι ενδιαφερόμενοι παρακαλούνται όπως υποβάλουν έγγραφη προσφορά, για το σύνολο της προμήθειας, που αποτελεί αντικείμενο της παρούσας πρόσκλησης όπως προσδιορίζεται ειδικότερα στις τεχνικές προδιαγραφές αυτής με τα εξής στοιχεία:

ΠΡΟΣΦΟΡΑ για

«Προμήθεια Αδειών Λειτουργίας για Πακέτο Λογισμικού Ασφαλείας»

Οι προσφορές πρέπει να υποβληθούν μέχρι την **Παρασκευή, 14 Μαΐου 2021 και ώρα 12:00 μμ** με τα στοιχεία της Πρόσκλησης, με έναν από τους παρακάτω τρόπους: Ηλεκτρονικά, στην ηλεκτρονική διεύθυνση: kopani@certh.gr ή μέσω ταχυδρομείου ή ταχυμεταφορέα (courier) στη διεύθυνση:

ΕΚΕΤΑ / ΙΝΕΒ Θεσσαλονίκη: 6ο χλμ. Χαριλάου-Θέρμης, 57001 Θέρμη Θεσσαλονίκης
Γραμματεία ΙΝΕΒ
Υπεύθυνος παραλαβής προσφορών: κα Κοπάνη Φωτεινή, τηλ. +30 2310498272

Για τη λήψη της τελικής απόφασης και επιλογής, μεταξύ των προσφορών που πληρούν τις τεχνικές προδιαγραφές της παρούσας Πρόσκλησης, θα συνεκτιμηθούν:

α) Το ύψος της οικονομικής προσφοράς
β) Η πληρότητα και αρτιότητα της πρότασης
γ) Η τεχνική και επαγγελματική ικανότητα των υποψηφίων
δ) Η διάρκεια εγγύησης (εφόσον παρέχεται)
ε) Η τεχνική υποστήριξη μετά την πώληση
στ) Η διαθεσιμότητα
ζ) Ο χρόνος παράδοσης

Η υποβολή της προσφοράς συνεπάγεται την πλήρη και ανεπιφύλακτη αποδοχή από τον υποψήφιο Ανάδοχο όλων των όρων της παρούσας πρόσκλησης.

Ο Ανάδοχος πριν την υπογραφή της σύμβασης ή την ανάθεση υποχρεούται να προσκομίσει:

α) Υπεύθυνη Δήλωση ότι δεν συντρέχουν για τον Ανάδοχο οι λόγοι αποκλεισμού του άρθρου 73 παρ. 1 του Ν. 4412/2016, όπως έχει τροποποιηθεί και ισχύει.
Η ως άνω Υπεύθυνη Δήλωση υπογράφεται, κατά περίπτωση, ως εξής:
i) Στην περίπτωση φυσικού προσώπου, από το φυσικό πρόσωπο, ii) Στην περίπτωση Ε.Π.Ε., Ι.Κ.Ε., Ο.Ε. και Ε.Ε. από τους διαχειριστές, iii) Στην περίπτωση Α.Ε. από τον εκπρόσωπό της. Ως εκπρόσωπος νοείται ο νόμιμος εκπρόσωπος αυτής, όπως προκύπτει από το ισχύον καταστατικό ή το πρακτικό εκπροσώπησής της κατά το χρόνο υποβολής της προσφοράς ή αίτησης συμμετοχής ή το αρμοδίως εξουσιοδοτημένο φυσικό πρόσωπο να εκπροσωπεί αυτήν για διαδικασίες σύναψης συμβάσεων ή για συγκεκριμένη διαδικασία σύναψης σύμβασης, iv) Σε κάθε άλλη περίπτωση νομικού προσώπου το/τους νόμιμο/ους εκπρόσωπο/ους του,[1]
β) Τελευταία τροποποίηση του καταστατικού της εταιρείας ή οποιοδήποτε άλλο επίσημο νομιμοποιητικό έγγραφο από το οποίο προκύπτει ο νόμιμος εκπρόσωπος της εταιρείας, εφόσον ο προσφέρων είναι νομικό πρόσωπο
γ) Φορολογική ενημερότητα σε ισχύ
δ) Ασφαλιστική ενημερότητα σε ισχύ
ε) Οποιοδήποτε άλλο δικαιολογητικό τυχόν ζητηθεί από την Αναθέτουσα Αρχή στα πλαίσια εφαρμογής της ισχύουσας περί δημοσίων συμβάσεων νομοθεσίας.

Τον Ανάδοχο βαρύνουν οι ακόλουθες κρατήσεις:
α) Ο προβλεπόμενος φόρος εισοδήματος
β) Κράτηση ύψους 0,06%, υπέρ της Αρχής Εξέτασης Προδικαστικών Προσφυγών (ΑΕΠΠ), η οποία επιβάλλεται επί της συνολικής αξίας κάθε αρχικής, τροποποιητικής ή συμπληρωματικής σύμβασης προ φόρων και κρατήσεων (άρθρο 350 παρ. 3 Ν. 4412/2016 & Κ.Υ.Α. 1191/2017 ΦΕΚ 969 Β΄/22-03-2017). Επί της παραπάνω κράτησης επιβάλλεται τέλος χαρτοσήμου 3%, πλέον εισφοράς υπέρ ΟΓΑ ποσοστού 20%, υπολογιζόμενου επί το τέλος χαρτοσήμου.
γ) Κράτηση ύψους 0,07% υπέρ της Ενιαίας Ανεξάρτητης Αρχής Δημοσίων Συμβάσεων (ΕΑΑΔΗΣΥ), η οποία υπολογίζεται επί της αξίας, χωρίς ΦΠΑ, της αρχικής και κάθε συμπληρωματικής σύμβασης (άρθρο 4 παρ. 3 του Ν. 4013/2011, όπως τροποποιήθηκε και ισχύει & Υ.Α. 3491/2017 ΦΕΚ Β 1992/9.6.2017). Επί της παραπάνω κράτησης επιβάλλεται τέλος χαρτοσήμου 3%, πλέον εισφοράς υπέρ ΟΓΑ ποσοστού 20%, υπολογιζόμενου επί το τέλος χαρτοσήμου.

Στοιχεία επικοινωνίας για πληροφορίες και διευκρινίσεις: Χουβαρδάς Βασίλειος τηλ. 2310 498479, email: vchou@certh.gr

Για το ΕΚΕΤΑ / ΙΝΕΒ

κ. Σταματόπουλος Κωνσταντίνος
Διευθυντής ΙΝΕΒ

[1] Η υποχρέωση της μη συνδρομής των λόγων αποκλεισμού της παραγράφου 1 του άρθρου 73 του Ν. 4412/2016 αφορά αα) στις περιπτώσεις Ε.Π.Ε., Ι.Κ.Ε. και προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.), τους διαχειριστές , ββ) στις περιπτώσεις ανωνύμων εταιρειών (Α.Ε.), τον Διευθύνοντα Σύμβουλο, καθώς και όλα τα μέλη του Διοικητικού Συμβουλίου

ΠΕΡΙΓΡΑΦΗ - ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΞΟΠΛΙΣΜΟΥ

Το Ινστιτούτο Εφαρμοσμένων Βιοεπιστημών (INEB) του Εθνικού Κέντρου Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ), για τις ανάγκες των ερευνητικών έργων «PVClinical – Ενεργή φαρμακοεπαγρύπνηση σε κλινικά περιβάλλοντα», Τ1ΕΔΚ-03789, κωδικός MIS 5032805 και «Take-A-Breath: Ευφυές σύστημα Αυτοδιαχείρισης και Υποστήριξης ασθενών με χρόνια Αναπνευστικά Προβλήματα», Τ1ΕΔΚ-03832, κωδικός MIS 5030881 πρόκειται να προμηθευτεί άδειες λειτουργίας για πακέτο λογισμικού ασφαλείας διάρκειας τριών ετών, σύμφωνα με τις τεχνικές προδιαγραφές που περιγράφονται, οι οποίες πρέπει να πληρούνται στο σύνολό τους.

ΠΕΡΙΓΡΑΦΗ: ΑΔΕΙΕΣ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

CPV: 48730000-4

Το υπό προμήθεια πακέτο λογισμικού αποτελείται από δύο (2) εκδόσεις του λογισμικού ως ακολούθως:

A. CheckPoint SandBlast Agent Advanced

Ποσότητα: 98 άδειες χρήσης διάρκειας τριών ετών

Α/Α	Προδιαγραφή	Απαίτηση	Απάντηση*	Παραπομπή**
1	Το λογισμικό θα πρέπει να ανιχνεύει και να αποτρέπει επιθέσεις από το exploitation στάδιο πριν ο κακόβουλος κώδικας εκτελεστεί.	ΝΑΙ		
2	Το λογισμικό θα πρέπει να εκτελεί το κακόβουλο αρχείο σε περιβάλλον sandbox για την ασφαλή κατηγοριοποίηση και αποτροπή του.	ΝΑΙ		
3	Το λογισμικό θα πρέπει να αποτρέπει πιθανές κακόβουλες επικοινωνίες από μολυσμένα τερματικά προς κακόβουλους servers προς το Internet (Command & Control servers).	ΝΑΙ		
4	Το λογισμικό θα πρέπει να μπορεί να σταματά επιθέσεις και επαναφέρει πιθανώς μολυσμένα τερματικά από κακόβουλα ή ransomware αρχεία.	ΝΑΙ		
5	Η λειτουργία anti-ransomware θα πρέπει να λειτουργεί ακόμη και σε περιπτώσεις που δεν είναι δυνατή η σύνδεση στο Internet.	ΝΑΙ		
6	Το λογισμικό θα πρέπει να προσφέρει λειτουργίες αποτροπής ηλεκτρονικού "ψαρέματος" (anti-phishing) με έλεγχο φορμών web για την ακεραιότητά τους.	ΝΑΙ		
7	Το λογισμικό θα πρέπει να προσφέρει λειτουργίες αποτροπής απώλειας εταιρικών κωδικών χρηστών (corporate credentials exposure).	ΝΑΙ		

8	Το λογισμικό θα πρέπει να ελέγχει αρχεία και να τα παραδίδει σε πραγματικό χρόνο στο χρήστη σε καθαρή μορφή, από όπου έχει αφαιρεθεί οποιοδήποτε κακόβουλο περιεχόμενο (file scrubbing).	ΝΑΙ		
9	Το λογισμικό θα πρέπει να παρέχει έλεγχο θυρών του συστήματος, αφαιρούμενων και περιφερειακών συσκευών.	ΝΑΙ		
10	Το λογισμικό θα πρέπει να παρέχει ενσωματωμένο VPN client για την ασφαλή σύνδεση φορητών συσκευών με τον οργανισμό.	ΝΑΙ		
11	Το λογισμικό θα πρέπει να παρέχει αναφορές και forensics με σκοπό τον έλεγχο της ασφάλειας των τερματικών και την ανεύρεση πιθανών περιστατικών ασφαλείας.	ΝΑΙ		
12	Το λογισμικό θα πρέπει να διαθέτει κεντρική κονσόλα διαχείρισης μέσω της οποίας θα υποστηρίζονται ο ορισμός πολιτικών ασφαλείας, η δημιουργία ομάδων χρηστών/συστημάτων, η καταγραφή των logs, η εγκατάσταση ενημερώσεων, η εξαγωγή αναφορών.	ΝΑΙ		
13	Θα πρέπει να είναι εφικτός ο ορισμός επιτρεπόμενων λιστών (whitelists) για την υλοποίηση εξαιρέσεων στη βασική πολιτική.	ΝΑΙ		
14	Το λογισμικό θα πρέπει να υποστηρίζει σταθμούς εργασίας (Η/Υ) είτε αυτοί βρίσκονται εντός της περιμέτρου είτε είναι απομακρυσμένοι.	ΝΑΙ		
15	Το λογισμικό θα πρέπει να παρέχει πρόσβαση στην κονσόλα διαχείρισης μέσω role-based λογαριασμών.	ΝΑΙ		
16	Το λογισμικό θα πρέπει να παρέχει τη δυνατότητα εξαιρέσεων με βάση αρχεία και φακέλους.	ΝΑΙ		
17	Το λογισμικό θα πρέπει να παρέχει τη δυνατότητα προσωρινής απενεργοποίησης συγκεκριμένων λειτουργιών σύμφωνα με τις ανάγκες του διαχειριστή.	ΝΑΙ		
18	Το λογισμικό θα πρέπει να υποστηρίζει κατ' ελάχιστο λειτουργικά συστήματα Windows 7 SP1, Windows 2008 R2, VDI, Linux.	ΝΑΙ		
19	Το λογισμικό θα πρέπει να έχει τη δυνατότητα να εκτελεστεί σε hypervisor.	ΝΑΙ		
20	Το λογισμικό θα πρέπει να παρέχει πληροφόρηση για την κατάσταση / Health του agent.	ΝΑΙ		

21	Το λογισμικό θα πρέπει να παράγει αναφορές οι οποίες απεικονίζουν γραφικά σε μορφή "δέντρου" τις δραστηριότητες του συστήματος με σκοπό την ευκολότερη διερεύνηση περιστατικών ασφαλείας. Να υποστηρίζεται αναπαράσταση των ευρημάτων σύμφωνα με το MITRE framework.	ΝΑΙ		
22	Το λογισμικό θα πρέπει να παρέχει τρόπους απομόνωσης ενός μολυσμένου συστήματος.	ΝΑΙ		
23	Το λογισμικό θα πρέπει να έχει τη δυνατότητα να εφαρμόζει μέτρα προστασίας και αποτροπής (block/prevent) κακόβουλης δραστηριότητας.	ΝΑΙ		
24	Το λογισμικό θα πρέπει να προσφέρει τη δυνατότητα απομακρυσμένης λήψης ενεργειών στα συστήματα (quarantine, reboot, isolate κ.α.) με σκοπό την ευκολότερη διαχείρισή τους.	ΝΑΙ		
25	Το λογισμικό θα πρέπει να αποτρέπει πάντα την απόπειρα απεγκατάστασης του agent από το χρήστη είτε αυτός έχει δικαιώματα administrator είτε όχι. Για να επιτραπεί η απεγκατάσταση θα ζητείται μυστικό συνθηματικό το οποίο έχει οριστεί στην αντίστοιχη πολιτική από το διαχειριστή του λογισμικού ασφαλείας.	ΝΑΙ		
26	Το λογισμικό θα πρέπει να ανιχνεύει παραπλανητικές ιστοσελίδες (phishing websites) και να αποτρέπει την καταχώρηση οποιωνδήποτε δεδομένων στις φόρμες που αυτές περιλαμβάνουν.	ΝΑΙ		
27	Το λογισμικό θα πρέπει να ανιχνεύει και να καταγράφει περιστατικά διαρροής εταιρικών κωδικών πρόσβασης χρηστών (corporate credentials exposure) προς τρίτα/προσωπικά sites.	ΝΑΙ		
28	Το λογισμικό θα πρέπει να υποστηρίζει λειτουργία sandboxing και μέσω αυτής, την αποτροπή κακόβουλων αρχείων.	ΝΑΙ		
29	Το λογισμικό θα πρέπει να υποστηρίζει τη μετατροπή των αρχείων που κατεβάζει ένας χρήστης σε ασφαλή αρχεία σε μορφή .pdf, απαλλαγμένα από κάθε κακόβουλο στοιχείο ή κώδικα μηδενικού χρόνου, σύμφωνα με την ορισμένη πολιτική.	ΝΑΙ		

30	Το λογισμικό θα πρέπει να υποστηρίζει τον καθαρισμό των αρχείων που κατεβάζει ένας χρήστης διατηρώντας τον αρχικό τους τύπο, απαλλάσσοντάς τα από κάθε κακόβουλο στοιχείο ή κώδικα μηδενικού χρόνου, σύμφωνα με την ορισμένη πολιτική.	ΝΑΙ		
31	Η διαχείριση του λογισμικού θα πρέπει να προσφέρεται ως managed cloud υπηρεσία.	ΝΑΙ		
32	Η διαχείριση του λογισμικού η οποία προσφέρεται ως managed cloud υπηρεσία θα πρέπει να υποστηρίζει διασύνδεση με Active Directory.	ΝΑΙ		
33	Θα πρέπει να υπάρχει δυνατότητα η πολιτική να υλοποιείται διακριτά με κανόνες σύμφωνα με το Active Directory.	ΝΑΙ		
34	Το λογισμικό θα πρέπει να περιλαμβάνει host firewall και application control λειτουργίες.	ΝΑΙ		
35	Το λογισμικό θα πρέπει να προσφέρεται με menu του agent στα Ελληνικά.	ΝΑΙ		

**Αναγράφεται η λέξη ΝΑΙ, εφόσον το προσφερόμενο Είδος καλύπτει την αντίστοιχη τεχνική προδιαγραφή - απαίτηση*
*** Αναγράφεται η σελίδα της Προσφοράς από όπου προκύπτει η συμμόρφωση με την αντίστοιχη τεχνική προδιαγραφή- απαίτηση*

B. CheckPoint Sandblast Agent Complete
Ποσότητα: 20 άδειες χρήσης διάρκειας τριών ετών

Α/Α	Προδιαγραφή	Απαίτηση	Απάντηση*	Παραπομπή**
1	Το λογισμικό θα πρέπει να ανιχνεύει και να αποτρέπει επιθέσεις από το exploitation στάδιο πριν ο κακόβουλος κώδικας εκτελεστεί.	ΝΑΙ		
2	Το λογισμικό θα πρέπει να εκτελεί το κακόβουλο αρχείο σε περιβάλλον sandbox για την ασφαλή κατηγοριοποίηση και αποτροπή του.	ΝΑΙ		
3	Το λογισμικό θα πρέπει να αποτρέπει πιθανές κακόβουλες επικοινωνίες από μολυσμένα τερματικά προς κακόβουλους servers προς το Internet (Command & Control servers).	ΝΑΙ		
4	Το λογισμικό θα πρέπει να μπορεί να σταματά επιθέσεις και επαναφέρει πιθανώς μολυσμένα τερματικά από κακόβουλα ή ransomware αρχεία.	ΝΑΙ		

5	Η λειτουργία anti-ransomware θα πρέπει να λειτουργεί ακόμη και σε περιπτώσεις που δεν είναι δυνατή η σύνδεση στο Internet.	ΝΑΙ		
6	Το λογισμικό θα πρέπει να προσφέρει λειτουργίες αποτροπής ηλεκτρονικού "ψαρέματος" (anti-phishing) με έλεγχο φορμών web για την ακεραιότητά τους.	ΝΑΙ		
7	Το λογισμικό θα πρέπει να προσφέρει λειτουργίες αποτροπής απώλειας εταιρικών κωδικών χρηστών (corporate credentials exposure).	ΝΑΙ		
8	Το λογισμικό θα πρέπει να ελέγχει αρχεία και να τα παραδίδει σε πραγματικό χρόνο στο χρήστη σε καθαρή μορφή, από όπου έχει αφαιρεθεί οποιοδήποτε κακόβουλο περιεχόμενο (file scrubbing).	ΝΑΙ		
9	Το λογισμικό θα πρέπει να παρέχει κρυπτογράφηση δίσκων και αφαιρούμενων συσκευών.	ΝΑΙ		
10	Το λογισμικό θα πρέπει να παρέχει έλεγχο θυρών του συστήματος, αφαιρούμενων και περιφερειακών συσκευών.	ΝΑΙ		
11	Το λογισμικό θα πρέπει να παρέχει ενσωματωμένο VPN client για την ασφαλή σύνδεση φορητών συσκευών με τον οργανισμό.	ΝΑΙ		
12	Το λογισμικό θα πρέπει να παρέχει αναφορές και forensics με σκοπό τον έλεγχο της ασφάλειας των τερματικών και την ανεύρεση πιθανών περιστατικών ασφαλείας.	ΝΑΙ		
13	Το λογισμικό θα πρέπει να διαθέτει κεντρική κονσόλα διαχείρισης μέσω της οποίας θα υποστηρίζονται ο ορισμός πολιτικών ασφαλείας, η δημιουργία ομάδων χρηστών/συστημάτων, η καταγραφή των logs, η εγκατάσταση ενημερώσεων, η εξαγωγή αναφορών.	ΝΑΙ		
14	Θα πρέπει να είναι εφικτός ο ορισμός επιτρεπόμενων λιστών (whitelists) για την υλοποίηση εξαιρέσεων στη βασική πολιτική.	ΝΑΙ		
15	Το λογισμικό θα πρέπει να υποστηρίζει σταθμούς εργασίας (Η/Υ) είτε αυτοί βρίσκονται εντός της περιμέτρου είτε είναι απομακρυσμένοι.	ΝΑΙ		
16	Το λογισμικό θα πρέπει να παρέχει πρόσβαση στην κονσόλα διαχείρισης μέσω role-based λογαριασμών.	ΝΑΙ		

17	Το λογισμικό θα πρέπει να παρέχει τη δυνατότητα εξαιρέσεων με βάση αρχεία και φακέλους.	ΝΑΙ		
18	Το λογισμικό θα πρέπει να παρέχει τη δυνατότητα προσωρινής απενεργοποίησης συγκεκριμένων λειτουργιών σύμφωνα με τις ανάγκες του διαχειριστή.	ΝΑΙ		
19	Το λογισμικό θα πρέπει να υποστηρίζει κατ' ελάχιστο λειτουργικά συστήματα Windows 7 SP1, Windows 2008 R2, VDI, Linux.	ΝΑΙ		
20	Το λογισμικό θα πρέπει να έχει τη δυνατότητα να εκτελεστεί σε hypervisor.	ΝΑΙ		
21	Το λογισμικό θα πρέπει να παρέχει πληροφόρηση για την κατάσταση/health του agent.	ΝΑΙ		
22	Το λογισμικό θα πρέπει να παράγει αναφορές οι οποίες απεικονίζουν γραφικά σε μορφή "δέντρου" τις δραστηριότητες του συστήματος με σκοπό την ευκολότερη διερεύνηση περιστατικών ασφαλείας και να υποστηρίζεται αναπαράσταση των ευρημάτων σύμφωνα με το MITRE framework.	ΝΑΙ		
23	Το λογισμικό θα πρέπει να παρέχει τρόπους απομόνωσης ενός μολυσμένου συστήματος.	ΝΑΙ		
24	Το λογισμικό θα πρέπει να έχει τη δυνατότητα να εφαρμόζει μέτρα προστασίας και αποτροπής (block/prevent) κακόβουλης δραστηριότητας.	ΝΑΙ		
25	Το λογισμικό θα πρέπει να προσφέρει τη δυνατότητα απομακρυσμένης λήψης ενεργειών στα συστήματα (quarantine, reboot, isolate κ.α.) με σκοπό την ευκολότερη διαχείρισή τους.	ΝΑΙ		
26	Το λογισμικό θα πρέπει να αποτρέπει πάντα την απόπειρα απεγκατάστασης του agent από το χρήστη είτε αυτός έχει δικαιώματα administrator είτε όχι. Για να επιτραπεί η απεγκατάσταση θα ζητείται μυστικό συνθηματικό το οποίο έχει οριστεί στην αντίστοιχη πολιτική από το διαχειριστή του λογισμικού ασφαλείας.	ΝΑΙ		
27	Το λογισμικό θα πρέπει να ανιχνεύει παραπλανητικές ιστοσελίδες (phishing websites) και να αποτρέπει την καταχώρηση οποιωνδήποτε δεδομένων στις φόρμες που αυτές περιλαμβάνουν.	ΝΑΙ		

28	Το λογισμικό θα πρέπει να ανιχνεύει και να καταγράφει περιστατικά διαρροής εταιρικών κωδικών πρόσβασης χρηστών (corporate credentials exposure) προς τρίτα/προσωπικά sites.	ΝΑΙ		
29	Το λογισμικό θα πρέπει να υποστηρίζει λειτουργία sandboxing και μέσω αυτής, την αποτροπή κακόβουλων αρχείων.	ΝΑΙ		
30	Το λογισμικό θα πρέπει να υποστηρίζει τη μετατροπή των αρχείων που κατεβάζει ένας χρήστης σε ασφαλή αρχεία σε μορφή .pdf, απαλλαγμένα από κάθε κακόβουλο στοιχείο ή κώδικα μηδενικού χρόνου, σύμφωνα με την ορισμένη πολιτική.	ΝΑΙ		
31	Το λογισμικό θα πρέπει να υποστηρίζει τον καθαρισμό των αρχείων που κατεβάζει ένας χρήστης διατηρώντας τον αρχικό τους τύπο, απαλλάσσοντάς τα από κάθε κακόβουλο στοιχείο ή κώδικα μηδενικού χρόνου, σύμφωνα με την ορισμένη πολιτική.	ΝΑΙ		
32	Η διαχείριση του λογισμικού θα πρέπει να προσφέρεται ως managed cloud υπηρεσία.	ΝΑΙ		
33	Η διαχείριση του λογισμικού η οποία προσφέρεται ως managed cloud υπηρεσία θα πρέπει να υποστηρίζει διασύνδεση με Active Directory.	ΝΑΙ		
34	Θα πρέπει να υπάρχει δυνατότητα η πολιτική να υλοποιείται διακριτά με κανόνες σύμφωνα με το Active Directory.	ΝΑΙ		
35	Το λογισμικό θα πρέπει να περιλαμβάνει host firewall και application control λειτουργίες.	ΝΑΙ		
36	Το λογισμικό θα πρέπει να προσφέρεται με menu του agent στα Ελληνικά.	ΝΑΙ		

**Αναγράφεται η λέξη ΝΑΙ, εφόσον το προσφερόμενο Είδος καλύπτει την αντίστοιχη τεχνική προδιαγραφή - απαίτηση*
*** Αναγράφεται η σελίδα της Προσφοράς από όπου προκύπτει η συμμόρφωση με την αντίστοιχη τεχνική προδιαγραφή- απαίτηση*

Όπου στις ανωτέρω προδιαγραφές κατονομάζεται ρητά ο κατασκευαστής κάποιου είδους, αυτό κρίνεται ως αναγκαία προϋπόθεση ώστε να εξασφαλιστεί η βέλτιστη συμβατότητα, απόδοση και ορθή λειτουργία των υπό προμήθεια αδειών χρήσης με την ήδη εγκατεστημένη υπολογιστική υποδομή του Ινστιτούτου.

Χρόνος Παράδοσης: Εντός τριάντα **(**30) ημερών από την υπογραφή της σύμβασης ή την ανάθεση της προμήθειας.

Προσφορές μπορούν να υποβληθούν μόνο για το σύνολο των ειδών και για τη ζητούμενη ποσότητα κάθε είδους.

Οι προσφορές οι οποίες θα πρέπει να πληρούν τις ανωτέρω προδιαγραφές, πρέπει να περιλαμβάνουν κατ' ελάχιστο τα παρακάτω:

- Αναλυτική περιγραφή των προσφερόμενων ειδών και των τεχνικών χαρακτηριστικών τους
- Τιμή προσφοράς χωρίς ΦΠΑ, τον αναλογούντα ΦΠΑ και τιμή προσφοράς με ΦΠΑ για το σύνολο των ειδών και για τη ζητούμενη ποσότητα κάθε είδους
- Περιγραφή για το χρόνο και τρόπο παράδοσης των ειδών