Προμήθεια συνόλου λύσεων υλικού και λογισμικού ασφάλειας						
ΣΧΟΛΙΑ ΔΙΑΒΟΥΛΕΥΣΗΣ ΜΕ ΜΟΝΑΔΙΚΟ ΑΡΙΘΜΟ 2023DIAB27171						
Α/Α	**ΟΝΟΜΑ**	**e-mail**	**ΑΡΘΡΟ**	**ΣΧΟΛΙΟ**	**ΑΛΛΑΓΕΣ**	**ΑΠΑΝΤΗΣΕΙΣ**
1	**Νίκος Χριστάκης**	nikos@multipoint-group.com	8.2.6.4 Λογισμικό διακυβέρνησης και ταξινόμησης δεδομένων (σελ. 95,96,97)	Θα θέλαμε να υποβάλουμε τα ακόλουθα χαρακτηριστικά που μπορούν να θεωρηθούν επωφελή για τον οργανισμό: 1. Η σάρωση δομημένων και μη δομημένων δεδομένων προσφέρει ευρύτερη χρήση του εργαλείου ταξινόμησης δεδομένων εντός του οργανισμού. 2. Ένα πλήρες ευρετήριο αναζήτησης σε όλα τα σύνολα δεδομένων και επιλεγμένα αποθετήρια δεδομένων προσφέρει ευελιξία και ακρίβεια για την εξοικονόμηση ενέργειας και την κατανάλωση δεδομένων. 3. Ο προσδιορισμός μη χρησιμοποιούμενων δεδομένων (stale data) στον οργανισμό και η δυνατότητα αρχειοθέτησης γύρω από τις πολιτικές διατήρησης δεδομένων προσφέρει στον οργανισμό τη δυνατότητα να επιτύχει πρόσθετες απαιτούμενες εργασίες από το ίδιο εργαλείο και να εξοικονομήσει χρόνο. 4. Η δυνατότητα διασύνδεσης με εργαλεία DLP (Προστασίας Απώλειας Δεδομένων) προσφέρει	**ΝΑΙ**	Τα σημεία 1 και 2 καλύπτονται από τα σημεία 10 και 11 του Πίνακα. Τα σημεία 3 και 5 ενσωματώθηκαν στη διακήρυξη (προδ. 12, 14) καθώς θεωρείται ότι κινούνται στην κατεύθυνση της συμβολής στη συμμόρφωση της ΑΑΔΕ σε υφιστάμενες ή μελλοντικές απαιτήσεις συμμόρφωσης ή με επιχειρησιακές απαιτήσεις για τη διαχείριση μη χρησιμοποιούμενων δεδομένων. Τα σημεία 4,6 ενσωματώθηκαν στη διακήρυξη ως επιθυμητή απαίτηση. Συγκεκριμένα προστέθηκαν οι προδιαγραφές 16,17.

				επεκτασιμότητα για μελλοντικές ανάγκες. 5. Η δυνατότητα χρήσης του εργαλείου Λογισμικού Διακυβέρνησης και Ταξινόμησης Δεδομένων για την εφαρμογή του άρθρου 17 του GDPR «δικαίωμα στη διαγραφή» προσφέρει μια πρόσθετη περίπτωση χρήσης από το ίδιο εργαλείο. 6. Η δυνατότητα χρήσης του εργαλείου Λογισμικό Διακυβέρνησης και Ταξινόμησης Δεδομένων για την απευθείας επισήμανση (tagging) δεδομένων για αποθετήρια on premises και cloud καλύπτει μελλοντικές ανάγκες και τη δυνατότητα προσθήκης ετικετών δεδομένων για άλλα εργαλεία και περιπτώσεις χρήσης.		
2	**Παναγιώτης Πανταζής**	panagiotis.pantazis@cyberark.com	Παρατήρηση 1. Σελίδα 41 - Παράγραφος Α.8 - Χρόνος ισχύος και αριθμός αδειών χρήσης	Οι σύγχρονες λύσεις IAM και PAM προσφέρονται ως Cloud υπηρεσία με τη μορφή της συνδρομής που εμπεριέχει στο κόστος όχι μόνο το δικαίωμα χρήσης του λογισμικού, αλλά επιπρόσθετα τη συντήρηση, αναβάθμιση και τη φιλοξενία σε Public Cloud π.χ. της AWS. Η επιβράβευση προσφορών για άδειες χρήσης απεριόριστης χρονικής διάρκειας με επιπλέον βαθμούς αποτρέπει ουσιαστικά τους υποψήφιους αναδόχους να συμπεριλάβουν στην προσφορά	**ΟΧΙ**	Η απαίτηση στο σχόλιο δεν γίνεται δεκτή καθώς οι λύσεις SaaS αποκλείονται λόγω της ανάγκης εγκατάστασης και αξιοποίησης της υποδομής g-cloud. *Η επιπλέον βαθμολογία για άδειες χρήσης απεριόριστης χρονικής διάρκειας εξυπηρετεί τα συμφέροντα της ΑΑΔΕ και παράλληλα εκτιμάται ότι δεν περιορίζει τον ανταγωνισμό καθώς δεν πρόκειται για απαίτηση ή*

				τους νέα, μοντέρνα και ασφαλή λογισμικά και να οδηγηθούν στην επιλογή παλαιοτέρων/παρωχημένων λύσεων που θα οδηγήσουν σε custom περιβάλλοντα που δεν θα μπορούν να αναβαθιστούν γρήγορα με αποτέλεσμα όχι μόνο την έκθεση του Φορέα σε νέου τύπου κυβερνοπεπιθέσεις, αλλά και μεγάλα κόστη upgrade μελλοντικά.		*προϋπόθεση συμμετοχής, ενώ και το ύψος της επιπλέον βαθμολόγησης δεν είναι καθοριστικό ώστε να διαμορφώνει από μόνο του ευνοϊκή συνολική βαθμολογία για ορισμένους συμμετέχοντες και αντίστοιχα δυσμενή για άλλους.*
3	**Παναγιώτης Πανταζής**	panagiotis.pantazis@cyberark.com	Παρατήρηση 2. Σελίδα 82 – Παράγραφος 8.2.4 – Λογισμικά και Άδειες Χρήσης - Είναι επιθυμητό οι άδειες χρήσης των λογισμικών να έχουν απεριόριστη διάρκεια. Σε κάθε περίπτωση, η προσφερόμενη αδειοδότηση θα έχει ισχύ και θα καλύπτει την περίοδο εγγύησης «Καλής Λειτουργίας».	Προτείνουμε να αξιολογηθεί θετικά η προσφορά των χρηστών με τη μορφή της συνδρομής που να περιέχει την άδεια χρήσης, τη συντήρηση, αναβάθμιση και hosting των συστημάτων για τους λόγους που αναφέρουμε στην Παρατήρηση 1.	**ΟΧΙ**	Δεν γίνεται αποδεκτή η πρόταση λόγω της υποχρεωτικής χρήσης του g-cloud σαν περιβάλλον φιλοξενίας (host environment).
4	**Παναγιώτης Πανταζής**	panagiotis.pantazis@cyberark.com	Παρατήρηση 3. Σελίδα 82 - Πίνακας 1 – 400 χρήστες Σύστημα PAM (Privileged Access Management)	Υπάρχουν και εξωτερικοί συνεργάτες που περιλαμβάνονται στους 400 χρήστες; Αν ναι, παρακαλούμε να διαχωρίσετε τους τύπους χρηστών (στελέχη ΑΑΔΕ και μη).	**ΟΧΙ**	Διευκρινίζεται ότι το σύνολο των χρηστών είναι υπάλληλοι της ΑΑΔΕ.

5	**Παναγιώτης Πανταζής**	panagiotis.pantazis@cyberark.com	Παρατήρηση 4. Σελίδα 85 - Παράγραφος 8.2.6.1 - Πίνακας 3: Λειτουργικές απαιτήσεις λογισμικού Identity & Access Rights Management (IAM) - #3 Το λογισμικό θα εγκατασταθεί σε υποδομή η οποία θα παραχωρηθεί από την Αναθέτουσα Αρχή.	Παρατηρούμε ότι οι συγκεκριμένη προδιαγραφή περιορίζει υπερβολικά τον ελεύθερο ανταγωνισμό και τον αριθμό των κατασκευαστών Identity & Access Management (IAM), ειδικά αυτών που ηγούνται της IAM βιομηχανίας (σύμφωνα με το Leaders Magic Quadrant της εταιρείας συμβουλων Gartner) των οποίων οι λύσεις θα μπορούσαν να γίνουν αποδεκτές, και οι οποίες δεν προσφέρουν λύση on-premise, μεταξύ αυτών και της CyberArk. Ως ένας από τους μεγαλύτερους κατασκευαστές συστημάτων IAM παγκοσμίως, προτείνουμε να επιτραπεί η αξιολόγηση Identity & Access Managemement/MFA/SSO συστημάτων που παρέχονται με τη μορφή Software as a Service, ειδικά από τη στιγμή που στο #6 ζητείται να δίδεται η δυνατότητα στον Φορέα να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM στις υποδομές Δημόσιου Νέφους της Microsoft και της Amazon. Προτείνουμε η συγκεκριμένη προδιαγραφή να αφαιρεθεί προκειμένου να έχετε την δυνατότητα να αξιολογήσετε και Native Cloud Συστήματα από τα οποία ο Φορέας μπορεί να αποκομίσει τα υψηλότερα δυνατά οφέλη, από σύγχρονες	**ΟΧΙ**	Δεν γίνεται αποδεκτή η πρόταση λόγω της υποχρεωτικής χρήσης του g-cloud σαν σαν περιβάλλον φιλοξενίας (host environment).

				πλατφόρμες, οι οποίες υιοθετούνται με αυξανόμενο ρυθμό από Κυβερνητικούς Οργανισμούς σε διεθνές επίπεδο διότι προσφέρουν μεγάλα πλεονεκτήματα όπως: -εμπεριέχουν νέες τεχνολογίες όπως AI και Machine Learning -ενσωματώνουν ολοκληρωμένες/βέλτιστες διαδικασίες και πρακτικές -διασφαλίζουν την απρόσκοπτη και συνεχή αναβαθμισιμότητα με αυτόματες και τακτικές ενημερώσεις που εγκαθιστά ο κατασκευαστής με στόχο να είναι πλήρως διασφαλισμένα από σύγχρονες κυβερνοπεπιθέσεις -προσφέρουν την απαιτούμενη ευελιξία μέσω του προγραμματιστικού περιβάλλοντος ανάπτυξης για την έγκαιρη προσαρμογή των οργανισμών στις καθημερινά μεταβαλλόμενες, νέες απειλές που αντιμετωπίζουν -εμπεριέχουν τους υπολογιστικούς πόρους που θα διασφαλίσουν την υψηλή απόδοση του συστήματος, επομένως θα προσφέρουν μειωμένα κόστη στον Φορέα -εξαλείφουν την ανάγκη για σύνθετα έργα μειώνοντας έτσι σημαντικά το συνολικό κόστος ιδιοκτησίας και όλα αυτά με ασφάλεια, αξιοπιστία και ευελιξία		

				διαχείρισης και ανάλυσης των ταυτοτήτων. Επιπρόσθετα προτείνουμε: -Να αξιολογηθει θετικά αρχιτεκτονική του κατασκευαστή λογισμικού που διαχειρίζεται όλους τους τύπους χρηστών, PAM και IAM σε μια ενοποιημένη πλατφόρμα και το ίδιο Administration Portal -Να ζητηθεί καταγραφή, έλεγχος (audit) και προστασία όλης της δραστηριότητας των χρηστών στις εφαρμογές web. -Να ζητηθεί αποθήκευση, πλήρης διαχείριση και sharing με ασφάλεια των διαπιστευτηρίων (credentials) επιχειρηματικών εφαρμογών (Password Panagement) -Να ζητηθεί αυτοματοποίηση της διαχείρισης ταυτοτήτων με ροές εργασίας χωρίς κώδικα (no-code workflows)		
6	**Παναγιώτης Πανταζής**	panagiotis.pantazis@cyberark.com	Παρατήρηση 5. Σελίδα 89 - Παράγραφος 8.2.6.2 - Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management)	Θεωρούμε ότι πρέπει να αξιολογηθεί θετικά λογισμικό που εμπεριέχει: -κοινή πλατφόρμα IAM & PAM -πλήρεις δυνατότητες API -out-of-the-box διασυνδέσεις με γνωστά συστήματα και εφαρμογές τρίτων κατασκευαστών -PAM Client που υποστηρίζει IAM authentication πρωτόκολλα (SAML, OPENID) Συνιστούμε επίσης:	**ΝΑΙ**	*Σχετικά με τις επιμέρους προτάσεις:* *- Οι δυνατότητες API θεωρείται ότι καλύπτονται από τις αναφορές στο 8.2.7.2.* *- Ενσωματώθηκαν επιθυμητές απαιτήσεις για τα σημεία 2, 3 (Πίνακας PAM σημεία 27 και 28) και 4 (Πίνακας γενικών λειτουργικών σημείο 12).* *- Το roadmap αφορά εν γένει*

				-να ζητηθεί και να αξιολογηθεί το Roadmap της προσφερόμενης πλατφόρμας -να αξιολογηθεί εκτός από την εμπειρία του οικονομικού φορέα όπως ζητείται στην Σελίδα 24, Παράγραφος Α2, και η εμπειρία του κατασκευαστή του λογισμικού και το αντίστοιχο πελατολόγιο, όχι μόνο εντός της χώρας αλλά και παγκοσμίως. Σε αντίθετη περίπτωση δύναται ο διαγωνισμός να οδηγήσει ακομα και σε custom λύσεις που δεν θα είναι αντιστοίχων δυνατοτήτων με έτοιμες/κορυφαίες λύσεις της αγοράς. -να επιτραπεί και να αξιολογηθεί θετικά η προσφορά Native Cloud PAM Συστημάτων για τους ίδιους λόγους που αναφέρουμε ανωτέρω, στην παρατήρηση 4.		*μελλοντικές βελτιώσεις και επεκτάσεις και προστέθηκε σχετική επιθυμητή απαίτηση στον γενικό πίνακα (κεφάλαιο 8.2.6 Λειτουργικές Απαιτήσεις, Πίνακας 2: Γενικές λειτουργικές απαιτήσεις των λογισμικών/ λύσεων)* - Έγινε προσαρμογή στο κεφάλαιο 8.2.4 στο οποίο αναφέρεται ότι δεν γίνονται αποδεκτές custom λύσεις. Στο ίδιο κεφάλαιο προστέθηκε αναφορά για τη δυνατότητα κοινής πλατφόρμας για την κάλυψη παραπάνω από μίας λύσης. - Ως προς τα native cloud συστήματα διευκρινίζεται ότι δε γίνονται αποδεκτά λόγω της ανάγκης εγκατάστασης και αξιοποίησης της υποδομής g-cloud.
7	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8.2.6.4 Λογισμικό διακυβέρνησης και ταξινόμησης δεδομένων (σελ. 95,96,97)	Εδώ περιγράφονται οι δυνατότητες δύο λύσεων με βάση τις βέλτιστες λύσεις της αγοράς. Μία λύση ταξινόμησης και μίας λύσης διακυβέρνησης. Θα επιθυμούσαμε να παρέχουμε δύο λύσεις ή εναλλακτικά να διαιρεθεί η απαίτηση σε δύο προτάσεις.	**ΝΑΙ**	Προστέθηκε πρόβλεψη στο κριτήριο αξιολόγησης Α.1 (τελευταίο bullet). Προστέθηκε συγκεκριμένη αναφορά στον γενικό πίνακα, σημείο 13 (κεφάλαιο 8.2.6 Λειτουργικές Απαιτήσεις, Πίνακας 2: Γενικές λειτουργικές απαιτήσεις των λογισμικών/ λύσεων)

8	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8.2.6.1 Λογισμικό Identity and Access Rights Management (IAM) για τον έλεγχο της πρόσβασης χρηστών στα πληροφοριακά συστήματα (σελ. 85,86,87,88,89)	Εδώ περιγράφονται οι δυνατότητες δύο λύσεων με βάση τις βέλτιστες λύσεις της αγοράς. Μία λύση Identity και μίας λύσης Access Rights Management. Θα επιθυμούσαμε να παρέχουμε δύο λύσεις ή εναλλακτικά να διαιρεθεί η απαίτηση σε δύο προτάσεις.	**ΝΑΙ**	Προστέθηκε πρόβλεψη στο κριτήριο αξιολόγησης Α.1 (τελευταίο bullet). Προστέθηκε συγκεκριμένη αναφορά στον γενικό πίνακα, σημείο 13
9	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8.2.6.2 Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management) (σελ. 92)	"Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (out of the box reports) κατ΄ελάχιστον για τα ακόλουθα: Συμμόρφωση με τη νομοθεσία για την προστασία προσωπικών δεδομένων". Μπορούμε να έχουμε περισσότερες λεπτομέρειες, π.χ. στα reports οι IPs να μην εμφανίζονται συνδυαστικά με τα usernames, τα PII δεδομένα να μην εμφανίζονται καθόλου στα reports κτλ.	**ΟΧΙ**	Έχει αλλαχθεί το σημείο αυτό βάσει του σχολίου 20.
10	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8.2.6.2 Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management) (σελ. 91)	"Δημιουργία ροών εργασίας της πρόσβασης λαμβάνοντας υπόψιν παραμέτρους όπως η ώρα, ημερομηνία, τοποθεσία ώστε να μπορεί να επιτραπεί η πρόσβαση σε πόρου". Ως τοποθεσία μπορεί να θεωρηθεί και η πρόσβαση μέσω συγκεκριμένης IP;	**ΟΧΙ**	Επιβεβαιώνεται η κατανόηση του οικ. Φορέα
11	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8.2.6.2 Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management) (σελ. 90)	Στο κείμενο αναφέρεται "Δυνατότητα λειτουργίας και με λύση PAM τρίτου κατασκευαστή". Δεν περιγράφεται επαρκώς η λειτουργικότητα που απαιτείται για τη λύση PAM τρίτου κατασκευαστή.	**ΝΑΙ**	Έγινε αναδιατύπωση ως εξής "Να αναφερθούν οι δυνατότητες διασύνδεσης με PAM τρίτου κατασκευαστή."

12	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 25)	Η απαιτηση: Στέλεχος πληροφορικής συστήματος PAM,Για 2ετή εμπειρία σε έργα χρήσης και διαχείρισης που περιλαμβάνουν την υλοποίηση, παραμετροποίηση ή/και παροχή Συστήματος Privileged Access Management (PAM).Το στέλεχος αυτό δεν είναι ευκολο να έχει δύο (2) χρονια εμπειρία στην τεχνολογία αυτή που είναι τόσο πρόσφατη	**ΟΧΙ**	Η παρατήρηση δεν γίνεται αποδεκτή καθώς εκτιμάται ότι για εταιρείες που δραστηριοποιούνται στον χώρο είναι εφικτή η εύρεση στελέχους με την εμπειρία που περιγράφεται στη διακήρυξη.
13	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24)	Η απαίτηση 3 αναφέρει : Δύο (2) έως τέσσερα (4) έργα παροχής υπηρεσιών κέντρου υπηρεσιών ασφάλειας (Security Operation Center - SOC), σε φορείς του δημοσίου ή του ιδιωτικού τομέα που διαθέτουν κρίσιμες υποδομές, συνολικού προϋπολογισμού ίσου η μεγαλύτερου με το 30% του προϋπολογισμό του Έργου χωρίς ΦΠΑ και χωρίς το δικαίωμα προαίρεσης. Παρακαλούμε πολύ όπως απαλειφθεί δεδομένου ότι περιορίζει πολύ τους συμμετέχοντες	**ΝΑΙ**	Έγινε προσαρμογή της απαίτησης 3 της παραγράφου 2.2.6 ώστε 1) να μειωθεί το ποσοστό στο 20% του προϋπολογισμού του Έργου και 2) να ενσωματωθεί ορισμός της κρίσιμης υποδομής ως υποσημείωση. Η εμπειρία ενός οικονομικού φορέα σε κρίσιμες υποδομές είναι σημαντική και υπάρχει ικανός αριθμός φορέων που τη διαθέτει.

14	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24)	Η Παράγραφος αναφέρει : «Τουλάχιστον ένα (1) έργο υλοποίησης IAM (Identity & Access Right Management), ένα (1) έργο υλοποίησης PAM (Privileged Access Management) και ένα (1) έργο υλοποίησης SIEM (Security Information and Event Management) σε φορέα αντίστοιχης δραστηριότητας με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα).» Παρακαλούμε πολύ να αναληφθεί η φράση «σε φορέα αντίστοιχης δραστηριότητας με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα» μιας και περιορίζει κατά πολύ τους συμμετέχοντες	**ΝΑΙ**	Έγινε προσαρμογή της απαίτησης της διακήρυξης με διαγραφή της αναφοράς σε "αντίστοιχης δραστηριότητας φορέα με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα)"
15	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24)	Η παράγραφος αναφέρει: «Τα έργα θα πρέπει να έχουν συνολικό προϋπολογισμό ίσου ή μεγαλύτερο του 50% του προϋπολογισμού του έργου μη συμπεριλαμβανομένου Φ.Π.Α και του δικαιώματος προαίρεσης. Σε κάθε ένα από τα ανωτέρω έργα θα πρέπει να τεκμηριώνεται και η παροχή υπηρεσιών εγκατάστασης, παραμετροποίησης και εκπαίδευσης.» Παρακαλούμε πολύ να αντικατασταθεί σε:	**ΝΑΙ**	Το σημείο αυτό τροποποιήθηκε σε "Τα έργα θα πρέπει να έχουν συνολικό προϋπολογισμό ίσου ή μεγαλύτερο του 30% του προϋπολογισμού του έργου μη συμπεριλαμβανομένου Φ.Π.Α και του δικαιώματος προαίρεσης. Σε κάθε ένα από τα ανωτέρω έργα θα πρέπει να τεκμηριώνεται και η παροχή υπηρεσιών εγκατάστασης,

				«Τα έργα θα πρέπει να έχουν συνολικό προϋπολογισμό ίσου ή μεγαλύτερο του 20% του προϋπολογισμού του έργου»		παραμετροποίησης και εκπαίδευσης."
16	**Oracle**	george.spiliotopoulos@oracle.com	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	Α) Στην παράγραφο 8.2.6.1 "Λογισμικό Identity and Access Rights Management (IAM) για τον έλεγχο της πρόσβασης χρηστών στα πληροφοριακά συστήματα" γίνεται αναφορά των τεχνικών απαιτήσεων / δυνατοτήτων που θα πρέπει να ικανοποιούνται από το προσφερόμενο λογισμικό Identity & Access Rights Management (IAM). Πέραν αυτού, κρίνουμε απαραίτητο να περιγράφουν σε μεγαλύτερη λεπτομέρεια οι πραγματικές και λειτουργικές απαιτήσεις που το προσδοκώμενο σύστημα IAM θα καλεστεί να εκπληρώσει. Επιπλέον τα στοιχεία που ζητούνται είναι απαραίτητα για την σωστή διαστασιολόγηση των υπηρεσιών του έργου που θα κληθεί ο ανάδοχος να υλοποιήσει (και δεν μπορεί να γίνει σε μετέπειτα στάδιο πχ. Μελέτη εφαρμογής) - Να δοθεί λίστα με τις εφαρμογές οι οποίες στα πλαίσια του έργου θα ενταχθούν στην πλατφόρμα IAM, τις δυνατότητες διασύνδεσης που παρέχει κάθε εφαρμογή (REST, web services, database access), την τεχνολογία (πχ Java, IIS), την	**ΝΑΙ**	Ως προς την παρατήρηση για την παροχή σε μεγαλύτερη λεπτομέρεια των πραγματικών και λειτουργικών απαιτήσεων για το IAM διευκρινίζεται ότι τα στοιχεία αυτά θα συλλεχθούν από τον Ανάδοχο με την υποστήριξη της ΑΑΔΕ κατά την εκπόνηση της Μελέτης Εφαρμογής. Η απαίτηση για δυνατότητα διασύνδεσης του IAM με περισσότερες από μια έμπιστες πηγές (που θα υποδειχθούν από την ΑΑΔΕ κατά τη φάση της Μελέτης Εφαρμογής) για την άντληση των στοιχείων ταυτοτήτων των χρηστών, ενσωματώθηκε στην διακήρυξη. *(κεφ. 8.2.6.1 νέα απαίτηση 10)* Η απαίτηση για δυνατότητα χρήσης LDAP virtualisation από την πλατφόρμα IAM δεν ενσωματώθηκε καθώς η πηγή αυθεντικοποίησης θα είναι μοναδική.

				έκδοση κάθε εφαρμογής (π.χ. Oracle Forms 11g) και τον τύπο της βάσης (π.χ. SQL Server 2019, Oracle 12c) - Σε ποιες από τις εφαρμογές αυτές θα ενεργοποιηθούν Single Sign-On (SSO), MFA και Access Management μηχανισμοί - Ποιες από τις εφαρμογές είναι web ή mobile ή client/server (εφαρμογές θα πρέπει να φορτωθούν στο IAM στα πλαίσια του έργου; - Σε περίπτωση που στα πλαίσια του έργου θα ενταχθεί και Σύστημα Διαχείρισης Ανθρωπίνου Δυναμικού, ενημερώστε μας αν είναι εμπορικό λογισμικό (π.χ. SAP HCM), σε ποια έκδοση του και ποια βάση (π.χ. SAP HANA, Oracle 12c) χρησιμοποιεί και αν αποθηκεύονται σε αυτό μόνο οι υπάλληλοι ΑΑΔΕ ή και οι εξωτερικοί συνεργάτες. - Ποια θα είναι η έμπιστη πηγή για τους εξωτερικούς συνεργάτες (μπορεί να καταχωρούνται και στο IAM από τις εκάστοτε μονάδες που τους διαχειρίζονται). - Πόσα είναι τα domains του Active Directory που θα πρέπει να διαχειρίζεται το IAM. - Πόσοι είναι οι LDAP που θα πρέπει να διαχειρίζεται το IAM, τι τύπου είναι (OUD, Open LDAP,…)		Ως προς το MFA της πλατφόρμας IAM, ενσωματώθηκε η απαίτηση για υποστήριξη αποστολής token με χρήση mobile authenticator συμβατού με το πρότυπο RFC-6238 ώστε να μπορούν να χρησιμοποιηθούν οι πιο γνωστοί mobile authenticators (Microsoft, Oracle, κτλ) καθώς και με SMS ή e-mail. *(κεφ. 8.2.6.1 προδιαγραφή 18)*

				και η έκδοση τους. - Ποιος ο αριθμός των εφαρμογών που χρησιμοποιούν AD groups για το authorization των χρηστών, είτε άμεσα, είτε έμμεσα (μέσω mapping 1-1 με local ρόλους της εφαρμογής). - Σε ποιες εφαρμογές Θα πρέπει να επιλεγούν οι πιο σημαντικές εφαρμογές (π.χ. SAP) για το role mining - Από τους 13700 χρήστες του IAM, πόσοι είναι υπάλληλοι ΑΑΔΕ και πόσοι εξωτερικοί συνεργάτες; Επιπλέον θεωρούμε ότι η πλατφόρμα IAM θα πρέπει αν έχει και τις παρακάτω δυνατότητες ώστε να ικανοποιούνται τελευταίας τεχνολογίας λειτουργικότητες και επίπεδα ασφάλειας (authentication) Β) Το IAM θα πρέπει να έχει δυνατότητα διασύνδεσης με περισσότερες από μια έμπιστες πηγές για την άντληση των στοιχείων ταυτοτήτων των χρηστών. Γ) Προτείνουμε το MFA της πλατφόρμας IAM, να μπορεί να υποστηρίζει την αποστολή tokens με χρήση mobile authenticator συμβατού με το πρότυπο RFC-6238 ώστε να μπορούν να χρησιμοποιηθούν οι πιο γνωστοί		

				mobile authenticators (Microsoft, Oracle, κτλ) καθώς και με SMS ή e-mail. Δ) Προτείνουμε η πλατφόρμα IAM να μπορεί να χρησιμοποιήσει περισσότερα από ένα identity stores τύπου LDAP για την αυθεντικοποίηση (authentication) των χρηστών, με χρήση LDAP virtualization έτσι ώστε ο authentication server αλλά και οι εφαρμογές που χρησιμοποιούν LDAP/AD να βλέπουν τους χρήστες κάτω από ένα LDAP tree. Αυτό θα δώσει την δυνατότητα σε πολλές εφαρμογές που μπορούν να διασυνδεθούν με έναν μόνο Lνα βλέπουν χρήστες από διαφορετικούς καταλόγους, κάτω από ένα δέντρο σε διαφορετικά OUs.		

17	Oracle	george.spiliotopoulos@oracle.com	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	1) Στην 2.2.6 Τεχνική και επαγγελματική ικανότητα στη σελίδα 24 και συγκεκριμένα στα σημεία Α1 η απαίτηση του υποψήφιου ανάδοχου αναφορικά με «την προμήθεια, εγκατάσταση και παραμετροποίηση συστήματος IAM (Identity & Access Rights Management)» θα πρέπει να γίνει πιο συγκεκριμένη, και να αφορά έργα που έχει ολοκληρώσει με την προσφερόμενη πλατφόρμα IAM με τα οποία θα συμμετάσχει στον διαγωνισμό. Το ίδιο να ισχύσει και στο σημείο Α2 όπου ζητείτε γενικά ο υποψήφιος ανάδοχος να έχει «2. Τουλάχιστον ένα (1) έργο υλοποίησης IAM (Identity & Access Right Management)» να γίνει ειδικό και να αναφέρετε συγκεκριμένα σε έργα που έχει ολοκληρώσει με την προσφερόμενη πλατφόρμα IAM με την οποία θα συμμετάσχει στον διαγωνισμό. 2) Επιπλέον στο ίδια άρθρο 2.2.6 Τεχνική και επαγγελματική ικανότητα στο σημείο Β στη σελίδα 25, η απαίτηση αφορά η ομάδα έργου να έχει μόνο ένα «Στέλεχος πληροφορικής συστήματος IAM, το οποίο να διαθέτει κατ’ ελάχιστο: - Πανεπιστημιακό Τίτλο (Πτυχίο ΑΕΙ ή ΑΤΕΙ) στην Πληροφορική ή σε	**ΝΑΙ**	Για την παρατήρηση στην παράγραφο 1, η απαίτηση παρέμεινε γιατί η προσαρμογή που ζητείται κρίνεται ότι δεν είναι προς το συμφέρον της ΑΑΔΕ. Για την παρατήρηση στην παράγραφο 2, προστέθηκε η απαίτηση "Εξαιρετική γνώση του προσφερόμενου προϊόντος, η οποία να βεβαιώνεται από τον κατασκευαστή." για το στέλεχος πληροφορικής συστήματος IAM. Για την παρατήρηση στην παράγραφο 3, η πρόταση του Οικονομικού Φορέα δεν γίνεται αποδεκτή. Συμφωνα με την έρευνα που έχει γίνει η διαστασιολόγηση είναι επαρκής.

				Τεχνολογίες Πληροφορικής και Επικοινωνιών ή Πανεπιστημιακό Τίτλο (Πτυχίο ΑΕΙ ή ΑΤΕΙ) θετικής/τεχνολογικής κατεύθυνσης, ή ισότιμοι τίτλοι σχολών της ημεδαπής ή αλλοδαπής. - 2ετή εμπειρία σε έργα που περιλαμβάνουν την υλοποίηση, παραμετροποίηση ή/ και παροχή Συστήματος Identity & Access Rights Management (IAM). Από την εμπειρία μας σε παρόμοιες υλοποιήσεις IAM ομοίου βεληνεκούς (13.700 χρηστών) που δυνητικά θα επηρεάσουν σε ένα βαθμό και την λειτουργία του φορέα, η ομάδα έργου οφείλει να αποτελείτε από έμπειρα στελέχη και για αυτό προτείνουμε η ομάδα έργου να αποτελείται από τουλάχιστον 4 μέλη με εμπειρία άνω των 5 ετών σε υλοποιήσεις με την προσφερόμενη πλατφόρμα λογισμικού IAM και όχι γενικά και αόριστα σε συστήματα IAM καθώς επίσης και κατ΄ελάχιστο 2 από τα μέλη να φέρουν και τις σχετικές πιστοποιήσεις του λογισμικού από τον κατασκευαστή (όπως σωστά ζητείτε στην ομάδα έργου για τις υπηρεσίες SOC) 3) Τέλος προτείνουμε στον Φορέα να εξετάσει την προσαύξηση του συνολικού προυπολογισμού του		

				έργου τουλάχιστον κατά 50% με σκοπό να παραλάβει μία πλήρως λειτουργική ή και ολοκληρωμένη λύση βασιζόμενη στις βέλτιστες πρακτικές υλοποίησης.		
18	NOVA ICT	tenders@novaict.gr	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	1) 8.2.14 Υπηρεσίες Security Operation Center (SOC) Προδ. 15 Σελ.110 «Με σκοπό τη δυνατότητα περαιτέρω διερεύνησης, ο ανάδοχος θα πρέπει να διαθέτει ομάδα αποκλειστικά για Threat Hunting και Forensic Investigation με δυνατότητα 24ωρης παροχής επιτόπου υποστήριξης εντός τριών (3) ωρών.» Σχόλιο Θεωρούμε πως η υπηρεσία Threat Hunting είναι ζωτικής σημασίας στην καθημερινή λειτουργία ενός SOC έτσι ώστε να υπάρχει και ενεργή πρόληψη αλλά και μείωση	**ΝΑΙ**	Η παρατήρηση ενσωματώθηκε στην προδιαγραφή 15 της υπηρεσίας SOC.

				των false positives. Γι' αυτό προτείνουμε τον διαχωρισμό των δύο υπηρεσιών έτσι ώστε η ίδια υπηρεσία να εμπλουτίζεται συνεχώς από τα αποτελέσματα Threat Hunting. Επιπλέον οι υπηρεσίες Forensic Investigation ίσως να μην χρειάζονται σε όλα τα περιστατικά και ως εκ τούτου θα μπορούσαν να προσφερθούν με ad-hoc 24ωρη υπηρεσία όταν είναι αναγκαίο. Με βάση τα παραπάνω προτείνουμε την αλλαγή της συγκεκριμένης παραγράφου ως εξής: «Με σκοπό τη δυνατότητα περαιτέρω διερεύνησης, ο ανάδοχος θα πρέπει να ενσωματώνει ενέργειες Threat Hunting σαν μέρος της 24ωρης παροχής SOC υπηρεσιών. Αυτές να αντικατοπτρίζονται σε οθόνες Threat Intelligence σαν μέρος του SIEM προϊόντος. Ο ανάδοχος να διαθέτει ομάδα αποκλειστικά για Forensic Investigation με δυνατότητα 24ωρης παροχής επιτόπου υποστήριξης εντός τριών (3) ωρών εφόσον και όταν χρειαστεί.»		

19	NOVA ICT	tenders@novaict.gr	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	2) 8.2.4 Λογισμικά ασφάλειας και Άδειες ΧρήσηςΠίνακας 1: Αριθμός αδειών χρήσης ανά λογισμικό Σελ. 82, 83Σύστημα SIEM (Security Information and Event Management), Μονάδα μέτρησηςΔιαστασιολόγησης Συσκευές, Ελάχιστος αριθμός 2508.2.6.3 Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας (SIEM)Προδ. 1 Σελ. 93 Υποστηριζόμενος όγκος αρχείων καταγραφής (log files) προσφερόμενης λύσης ανά ημέρα ≥ 20 GBΠίνακας Α Οικονομικής Προσφοράς Προμήθειας Έτοιμου ΛογισμικούΣειρά 3. Σύστημα SIEM (Security Information and Event Management) ΠΟΣΟΤΗΤΑ (άδειες χρήσης)ΣχόλιοΌπως διαπιστώνουμε στο τεύχος της διαβούλευσης ζητείται αδειοδότηση του λογισμικού SIEM με βάση τις συσκευές από τις οποίες θα δέχεται input. Οι περισσότερες λύσεις SIEM αδειοδοτούνται είτε βάση όγκου αρχείων καταγραφής (log files), είτε βάση Events per Second (EPS) και ανεξαρτήτως συσκευών. Επιπλέον η αδειοδότηση με συσκευές απαιτεί και αναλυτική παρουσίαση τους στα πλαίσια της διακήρυξης αφού μια φυσική συσκευή μπορεί να εμπεριέχει πολλαπλά διαφορετικά	**ΟΧΙ**	Διευκρινίζεται ότι τα στοιχεία θα συλλεχθούν από τον ανάδοχο με την υποστήριξη της ΑΑΔΕ κατά τη Μελέτη Εφαρμογής.

				sources τα οποία δίνουν πληροφορίες στο SIEM. Προτείνουμε λοιπόν να αλλαχθεί ο Πίνακας 1: Αριθμός αδειών χρήσης ανά λογισμικό και να δοθεί η δυνατότητα στους φορείς να αδειοδοτήσουν το λογισμικό SIEM είτε βάση του όγκου των 20 GB σε log files που αναφέρεται στη προδιαγραφή 1 είτε βάση του αντίστοιχου αριθμού EPS (Events per Second) με αντίστοιχη προσαρμογή του Πίνακα Α Οικονομική Προσφορά Προμήθειας Έτοιμου Λογισμικού.		
20	NOVA ICT	tenders@novaict.gr	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	3) 8.2.6.2 Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management) Προδ. 24 Σελ. 92 «Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (out of the box reports) κατ΄ελάχιστον για τα ακόλουθα: • Δραστηριότητα χρηστών ή ομάδων χρηστών • Δραστηριότητα σχετικά με τους κωδικούς πρόσβασης • Κατάσταση αιτημάτων έγκρισης και εγκριτικών ροών εργασίας • Εντοπισμός προνομιούχων λογαριασμών • Συμμόρφωση με τη νομοθεσία	**ΝΑΙ**	Έγινε ενσωμάτωση της παρατήρησης με σχετική προσαρμογή στην διακήρυξη (προδιαγραφή 24 του 8.2.6.2).

				για την προστασία προσωπικών δεδομένων» Σχόλιο Οι λύσεις PAM με την παροχή analytics & reporting δίνουν δυνατότητες παραγωγής αναφορών οι όποιες μπορούν να τεκμηριώσουν την συμμόρφωση με την νομοθεσία για προστασία προσωπικών δεδομένων. Δεν είναι όμως μια μεμονωμένη αναφορά out of the Box. θα προτείναμε η προδιαγραφή να αλλάξει ως παρακάτω : «Καταγραφή του συνόλου των γεγονότων του συστήματος και παραγωγή έτοιμων αναφορών (out of the box reports) κατ΄ελάχιστον για τα ακόλουθα: • Δραστηριότητα χρηστών ή ομάδων χρηστών • Δραστηριότητα σχετικά με τους κωδικούς πρόσβασης • Κατάσταση αιτημάτων έγκρισης και εγκριτικών ροών εργασίας • Εντοπισμός προνομιούχων λογαριασμών Να αποδειχθεί πως με την χρήση των αναφορών δύναται να τεκμηριωθεί η συμμόρφωση με τη νομοθεσία για την προστασία προσωπικών δεδομένων.»		

21	NOVA ICT	tenders@novaict.gr	ΤΕΥΧΟΣ ΔΙΑΚΗΡΥΞΗΣ	4) Άρθρο 2.2.9.2 Αποδεικτικά μέσα / Β.4.Α. Σελ. 34 Σχόλιο Σύμφωνα με το αντικείμενο του έργου το οποίο περιλαμβάνει «Προμήθεια λογισμικών για την ασφάλεια πληροφοριών», ενδέχεται τα έργα του ιδιωτικού τομέα, που έχουν υλοποιηθεί, να περιλαμβάνουν απόρρητες ή εμπιστευτικές πληροφορίες (επιχειρηματικές πληροφορίες που δεν μπορούν να αποκαλυφθούν λόγω εμπορικού απορρήτου) και επομένως δεν δύναται να αποκαλυφθούν ή δημοσιευθούν, καθώς προστατεύονται από συμφωνητικά εμπιστευτικότητας με τον πελάτη. Λόγω αυτής της ιδιαιτερότητας του υπό διαβούλευση έργου, παρακαλούμε όπως εξετάσετε την αλλαγή της απαίτησης της διακήρυξης σύμφωνα με το άρθρο 2.2.9.2 Αποδεικτικά μέσα / Β.4.Α. Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6.Α. "... να υποβάλλεται ως στοιχείο τεκμηρίωσης αντίγραφο της σύμβασης ή του σχετικού παραστατικού (τιμολόγιο) ..." και να αρκεί η υποβολή είτε Υπεύθυνης Δήλωσης του νόμιμου εκπροσώπου του ιδιώτη ή του οικονομικού	**ΝΑΙ**	Έγινε ενσωμάτωση της παρατήρησης με διαγραφή της απαίτησης για την παροχή αντιγράφου της σύμβασης ή του σχετικού παραστατικού (τιμολογίου).

				φορέα, είτε Βεβαίωση καλής εκτέλεσης του νόμιμου εκπροσώπου του ιδιώτη, δικαιολογητικό το οποίο επαναλαμβάνεται στις διακηρύξεις δημοσίων διαγωνισμών και η οποία θα περιλαμβάνει τα απαραίτητα στοιχεία που δύναται να γνωστοποιεί στην αναθέτουσα αρχή (και σε κάθε περίπτωση όσα απαιτούνται από τη Διακήρυξη), έτσι ώστε να υπάρχει ισορροπία μεταξύ της προστασίας των εμπιστευτικών πληροφοριών του πελάτη αλλά και προάσπιση των δικαιωμάτων του οικονομικού φορέα που επιθυμεί να υποβάλλει προσφορά.		

22	**Πάνος Παπανικολάου**	salesgr@odysseycs.com	ΔΙΑΚΗΡΥΞΗ	α. Άρθρο 8.2.6.2 Λογισμικό διαχείρισης προσβάσεων προνομιακών λογαριασμών (Privileged Access Management) Προδιαγραφή 18 «Αυτοματοποιημένη παροχή λογαριασμού για νέους χρήστες και αυτόματη ακύρωσή του όταν οι χρήστες αποχωρούν από την ΑΑΔΕ ή αλλάζουν θέσεις εργασίας. Για τον σκοπό αυτό το σύστημα PAM πρέπει να έχει δυνατότητα διαλειτουργικότητας με συστήματα Identity Management , όπως π.χ. συστήματα LDAP» Οι λύσεις PAM έχουν την δυνατότητα με αυτοματοποιημένο τρόπο να ανακαλύπτουν τους νέους λογαριασμούς και να τους εντάσσουν στο σύστημα με βάση τους κανόνες και πολιτικές που έχει ορίσει ο διαχειριστής. Η αυτόματη διαγραφή αποφεύγεται ώστε να μην χαθεί το ιστορικό πρόσβασης του χρήστη το οποίο θα χρειαστεί για την διαδικασία reporting ή και συμμόρφωσης. Τα λογισμικά PAM συνεργάζονται με συστήματα Identity και σε περίπτωση αλλαγής θέσης ή αποχώρησης μπορούν να αλλάξουν τα δικαιώματα του χρήστη εμποδίζοντας την πρόσβαση. Αποφεύγεται όμως η αυτόματη διαγραφή του χρήστη χωρίς να δοθεί συγκατάθεση από	**ΝΑΙ**	Ως προς το σημείο α του σχολίου που αφορά τη δυνατότητα ανακάλυψης με αυτοματοποιημένο τρόπο των νέων λογαριασμών η προδιαγραφή άλλαξε σύμφωνα με την πρόταση του οικονομικού φορέα. Ως προς το σημείο β του σχολίου που σχετίζεται με το άρθρο 2.2.7, αφαιρέθηκε η απαίτηση που σχετίζεται με τα "πεδία εφαρμογής παροχής συμβουλευτικών υπηρεσιών και υπηρεσιών πληροφορικής." Ως προς το σημείο γ του σχολίου που σχετίζεται με το άρθρο 2.2.6, έχει απαλειφθεί η ειδική εμπειρία του Υπευθύνου του Έργου και θα αυξηθεί η γενική εμπειρία.

				τον διαχειριστή. θα προτείναμε η προδιαγραφή να αλλάξει ως παρακάτω: «Αυτοματοποιημένη παροχή λογαριασμού για νέους χρήστες και αυτόματη αλλαγή των δικαιωμάτων του όταν οι χρήστες αποχωρούν από την ΑΑΔΕ ή αλλάζουν θέσεις εργασίας. Για τον σκοπό αυτό το σύστημα PAM πρέπει να έχει δυνατότητα διαλειτουργικότητας με συστήματα Identity Management , όπως π.χ. συστήματα LDAP.» β. Άρθρο 2.2.7 Πρότυπα διασφάλισης ποιότητας και πρότυπα περιβαλλοντικής διαχείρισης «Οι οικονομικοί φορείς για την παρούσα διαδικασία σύναψης σύμβασης οφείλουν να συμμορφώνονται με τα παρακάτω πρότυπα διασφάλισης ποιότητας: i) ISO 9001:2015 για τη Διαχείριση της Ποιότητας ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό, στα πεδία εφαρμογής παροχής συμβουλευτικών υπηρεσιών και υπηρεσιών πληροφορικής. ii) ISO 27001:2013 για την Ασφάλεια των Πληροφοριών ή ισοδύναμο, εν ισχύ, από διαπιστευμένο οργανισμό, στα		

				πεδία εφαρμογής παροχής συμβουλευτικών υπηρεσιών και υπηρεσιών πληροφορικής.» Δεδομένου ότι σύμφωνα με το άρθρο 8.2 Αντικείμενο του Έργου, στο αντικείμενο του έργου δεν ζητείται παροχή συμβουλευτικών υπηρεσιών, προτείνεται η αφαίρεση της απαίτησης στα πεδία εφαρμογής των προτύπων διασφάλισης ποιότητας, ISO 9001:2015 και ISO 27001:2013 (άρθρο 2.2.7) για το αντικείμενο " παροχής συμβουλευτικών υπηρεσιών" καθώς δεν υπάρχει συσχέτιση με το αντικείμενο του έργου. γ. Άρθρο 2.2.6 Τεχνική και επαγγελματική ικανότητα «Να διαθέτουν Ομάδα Έργου με στελέχη επαρκή σε πλήθος και δεξιότητες για την επιτυχή υλοποίηση του Έργου, η οποία να αποτελείται τουλάχιστον από: ο Υπεύθυνο Έργου, ο οποίος να διαθέτει κατ’ ελάχιστο: 10ετή εργασιακή εμπειρία στον σχεδιασμό και την υλοποίηση έργων πληροφορικής, συμπεριλαμβανομένης εμπειρίας σε διαχείριση τουλάχιστον πέντε (5) έργων που περιλαμβάνουν συστήματα ασφαλείας		

				πληροφοριακών συστημάτων συναφή με αυτά που περιλαμβάνονται στο αντικείμενο του έργου.» Δεδομένου ότι στη ζητούμενη Ομάδα Έργου υπάρχουν τόσο ο Τεχνικός Υπεύθυνος Έργου όσο και Έμπειρα Στελέχη στην υλοποίηση λύσεων πληροφορικής για την ασφάλεια πληροφοριών και την παροχή υπηρεσιών για την ασφάλεια πληροφοριών θεωρούμε ότι είναι σημαντική και επαρκής η συνολική εμπειρία για τον Υπεύθυνο Έργου και ως εκ τούτου προτείνουμε την αλλαγή της απαίτησης της διακήρυξης σε: ο Υπεύθυνο Έργου, ο οποίος να διαθέτει κατ' ελάχιστο: 10ετή εργασιακή εμπειρία στη διαχείριση, σχεδιασμό και την υλοποίηση έργων πληροφορικής.		
23	**NEUROSOFT**	m.xylogiannopoulos@neurosoft.gr	Διακήρυξη	Παρακαλούμε πολύ όπως δοθεί παράταση ως προς την καταληκτική ημερομηνία υποβολής σχολίων/ παρατηρήσεων για 2 εβδομάδες	**ΟΧΙ**	Έχει ικανοποιηθεί

				δεδομένου της πολυπλοκότητας του έργου.		
24	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	Παρακαλούμε πολύ όπως δοθεί παράταση ως προς την καταληκτική ημερομηνία υποβολής σχολίων/ παρατηρήσεων για 2 εβδομάδες δεδομένου της πολυπλοκότητας του έργου, των τεχνικών απαιτήσεων αλλά και της παραγράφου 2.2.6 Τεχνική και επαγγελματική ικανότητα η οποία είναι ιδιαίτερα απαιτητική και θέλει μελέτη - ειδικά οι παράγραφοι Α και Γ.	**ΟΧΙ**	Έχει ικανοποιηθεί
25	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ Στην 8.1.2.1 Αρχιτεκτονική Υποδομής Φιλοξενίας, στις δικτυακές απαιτήσεις λειτουργίας αναφέρεται: «διαστασιολόγηση ως προς τις δικτυακές απαιτήσεις των συστημάτων και ειδικότερα σε επίπεδο bandwidth και QoS. Ενδεικτικά: εκτιμώμενος ημερήσιος όγκος διακινούμενων δεδομένων ή αναφορά άλλης παραμέτρου που κρίνετε αναγκαία.» Ωστόσο, στην περίπτωση που ζητηθούν VMs από το on-premise Υπολογιστικό Νέφος που διαχειρίζεται η ΓΓΠΣ & ΨΔ, θα ζητηθεί συγκεκριμένο προτείνουμε πορτών, και καθώς η συγκεκριμένη περιγραφή ωθεί αποκλειστικά στην πρόταση μόνο λύσης στο Azure,	**ΝΑΙ**	Διευκρινίζεται ότι οι λύσεις θα φιλοξενηθούν στο Microsoft Azure. Έχει προσαρμοστεί η διακήρυξη και έχει αφαιρεθεί οποιαδήποτε αναφορά σε On-premises υποδομή.

				προτείνουμε να αλλαχθεί σε «Να αναφερθούν οι δικτυακές απαιτήσεις λειτουργίας της προσφερόμενης λύσης».		
26	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ: Στην παράγραφο 8.2.6, Γενικές Λειτουργικές Απαιτήσεις των Λογισμικών/λύσεων, Απαίτηση 3 αναφέρεται: «Τα λογισμικά/λύσεις θα πρέπει να είναι συμβατά με την τελευταία έκδοση του προτύπου ITIL (διαδικασίες, ρόλοι κλπ), κατ' ελάχιστο με την έκδοση 4.» Επειδή δεν υπάρχει επίσημη λίστα συμβατότητας εργαλείων με ITIL v4 προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ: Στην παράγραφο 8.2.6, Γενικές Λειτουργικές Απαιτήσεις των Λογισμικών/λύσεων, Απαίτηση 10 αναφέρεται: «Τα λογισμικά θα παρέχουν έναν μηχανισμό παρακολούθησης του βαθμού χρήσης των υπηρεσιών/εργαλείων από τους χρήστες και θα παράγει σχετικές ενημερώσεις στους διαχειριστές σε πραγματικό (real-time) και συσσωρευμένο (accumulated) χρόνο.» Καθώς η έννοια του «πραγματικού	**ΝΑΙ**	Το σχόλιο που σχετίζεται με την απαίτηση 3 της παραγράφου 8.2.6 δεν θα ενσωματωθεί καθώς κρίνεται ότι θα είναι χρήσιμη για τη συνεργασία κατά την υλοποίηση του έργου. Το σχόλιο που σχετίζεται με την απαίτηση 10 της παραγράφου 8.2.6 δεν θα ενσωματωθεί καθώς η εγκατάσταση της εφαρμογής θα πραγματοποιηθεί στο g-cloud και η εν λόγω λειτουργικότητα θεωρείται σημαντική για τους διαχειριστές. Το σχόλιο που σχετίζεται με την απαίτηση 11 της παραγράφου 8.2.6 ενσωματώθηκε σύμφωνα με την πρόταση του οικονομικού φορέα.

				χρόνου (real-time)» καθοδηγεί σε λύσεις cloud ενώ ο διαγωνισμός επιτρέπει και on-premise υλοποιήσεις, προτείνουμε να αφαιρεθεί ο όρος «σε πραγματικό (real-time) και συσσωρευμένο (accumulated) χρόνο.» ΕΡΩΤΗΣΗ: Στην παράγραφο 8.2.6, Γενικές Λειτουργικές Απαιτήσεις των Λογισμικών/λύσεων, Απαίτηση 11 αναφέρεται: “Η γραφική διεπαφή χρήστη κάθε επιμέρους λογισμικού/λύσης θα πρέπει να είναι συμβατή με σύγχρονα σχεδιαστικά πρότυπα και τεχνολογίες” Επειδή ο όρος «σύγχρονα σχεδιαστικά πρότυπα και τεχνολογίες» δεν μπορεί να αιτιολογηθεί, προτείνουμε να αλλαχθεί σε «γραφική διεπαφή χρήστη η οποία θα έχει ως γνώμονα τη φιλικότητα χρήσης, ανάγνωσης και αξιοποίησης του συνόλου της πληροφορίας από την ίδια κονσόλα».		

27	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ: Στην Παράγραφο 8.2.6.1, στις Λειτουργικές απαιτήσεις λογισμικού IAM, στην προδιαγραφή 6 αναφέρεται: Οι προσφερόμενες άδειες χρήσης λογισμικού της πλατφόρμας IAM θα επιτρέπουν στον Φορέα εάν το επιθυμεί να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM σε υ¬πο¬δομές Public Cloud. Η προσφερόμενη λύση θα πρέπει να μπορεί να μεταφερθεί και να λειτουργήσει κατ' ελάχιστων στις ακόλουθες υποδομές Δημόσιου Νέφους (Public Cloud Infrastructure): α)Microsoft Azure, β) Amazon Web Services. Καθώς, όπως είναι ξεκάθαρο από το παράρτημα V, οι υποδομές που χρησιμοποιεί ο φορέας είναι είτε στο Microsoft Azure είτε on-premise, η αναφορά στο AWS θεωρείτε περιττή και προτείνουμε να αφαιρεθεί.	**ΌΧΙ**	Η απαίτηση που υπάρχει ήδη στη διακήρυξη διατηρήθηκε καθώς προστατεύει τα συμφέροντα της ΑΑΔΕ στο μέλλον.

28	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ Στη παράγραφο 8.2.6.2, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (PAM) στην προδιαγραφή 1 αναφέρεται: Το λογισμικό PAM πρέπει να παρέχει δυνατότητα διαχείρισης της προνομιακής πρόσβασης σε ευρύ φάσμα συστημάτων και υποδομών, όπως λειτουργικά συστήματα, βάσεις δεδομένων, middleware, εφαρμογές, συσκευές δικτύου και υπηρεσίες Cloud και να λειτουργούν ως on premise υποδομή, υποδομή ως υπηρεσία (IaaS), πλατφόρμα ως υπηρεσία (PaaS), λογισμικό ως υπηρεσία (SaaS), ή συνδυασμό τους σε υβριδικά μοντέλα ανάπτυξης. Καθώς η ταυτόχρονη υλοποίηση σε on-premise, IaaS, PaaS, SaaS είναι αδύνατη και η υπόσταση αυτής της προδιαγραφής δεν έχει λογική προτείνουμε να μείνουν μόνο οι επιλογές για on-premise, IaaS και SaaS ή συνδυασμού για υβριδικό μοντέλο υλοποίησης. ΕΡΩΤΗΣΗ Στη παράγραφο 8.2.6.2, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών	**ΌΧΙ**	Το σχόλιο που σχετίζεται με την προδιαγραφή 1 της παραγράφου 8.2.6.2, δεν ενσωματώθηκε καθώς η αναφορά προστατεύει τα συμφέροντα της ΑΑΔΕ στο μέλλον. Το σχόλιο που αναφέρεται στην προδιαγραφή 6 "Δυνατότητα λειτουργίας και με λύση PAM τρίτου κατασκευαστή" της παραγράφου 8.2.6.2, η απαίτηση διατηρήθηκε για να καλύψει τυχόν περιπτώσεις διασύνδεσης με PAM άλλου φορέα. Το σχόλιο που αναφέρεται στην προδιαγραφή 6 "Πρόσβαση με χρήση agent (windows, mac, linux) και με HTML5" της παραγράφου 8.2.6.2, η απαίτηση διατηρήθηκε καθώς η πρόσβαση μέσω agent συμβάλλει στην ασφάλεια και τη δυνατότητα ιχνηλάτησης, ενώ η πρόσβαση με HTML5 συμβάλει στη φιλικότητα, την ενίσχυση της ασφάλειας και την προσβασιμότητα.

				(PAM) στην προδιαγραφή 6 αναφέρεται: Δυνατότητα λειτουργίας και με λύση PAM τρίτου κατασκευαστή. Καθώς ο φορέας θα έχει μόνο μία λύση PAM και καθώς δεν αναφέρεται συγκεκριμένα ο τρίτος κατασκευαστής, προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ Στη παράγραφο 8.2.6.2, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (PAM) στην προδιαγραφή 6 αναφέρεται: Πρόσβαση με χρήση agent (windows, mac, linux) και με HTML5 Καθώς η προδιαγραφή αυτή περιορίζει την πρόταση διεθνών αναγνωρισμένων λύσεων PAM που θεωρούνται leaders από τη Gartner καθώς γίνεται αρκετά συγκεκριμένη με τη χρήση agents και HTML5 προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ Στη παράγραφο 8.2.6.2, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (PAM) στην προδιαγραφή 6 αναφέρεται:		Το σχόλιο που αναφέρεται στην προδιαγραφή 6 "Δυνατότητα για δημιουργία ξεχωριστού portal ανά vendor με δυνατότητα διαχείρισης από εκπρόσωπό του.", η απαίτηση διατηρήθηκε καθώς η πρόσβαση από διαφορετικά portals μπορεί να έχει αξία στο μέλλον για την πρόσβαση εξωτερικών λογιαρισμών.

				Δυνατότητα για δημιουργία ξεχωριστού portal ανά vendor με δυνατότητα διαχείρισης από εκπρόσωπό του. Η συγκεκριμένη προδιαγραφή δεν έχει λογική καθώς η χρήση της λύσης PAM θα γίνει από τον φορέα επομένως δεν έχει λογική η δημιουργία πολλαπλών portal. Για το λόγο αυτό προτείνουμε να αφαιρεθεί.		
29	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ Στη παράγραφο 8.2.6.2, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (PAM) στην προδιαγραφή 6 αναφέρεται: Πλήρης υποστήριξη web interface υποδομών όπως: o Amazon Web Services o Google Cloud o VMware vSphere o Citrix XenServer	**ΌΧΙ**	Η διατύπωση παρέμεινε ως έχει καθώς προστατεύει τα συμφέροντα της ΑΑΔΕ στο μέλλον.

				o Microsoft Hyper-V o Microsoft Azure o IBM Softlayer o Rackspace Καθώς ο φορέας, όπως αναφέρεται και στο παράρτημα V, δεν χρησιμοποιεί όλες αυτές τις τεχνολογίες ενώ η απαίτηση για πρόσβαση στο web interface από browser είναι αρκετή προτείνουμε να αφαιρεθεί.		
30	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗΣτην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 1 αναφέρεται:• Υποστηριζόμενο throughput προσφερόμενης λύσης ≥ 3 Gbps• Υποστηριζόμενος όγκος αρχείων καταγραφής (log files) προσφερόμενης λύσης ανά ημέρα ≥ 20 GBΓια να μπορέσει ο φορέας να αξιοποιήσει τη λύση SIEM στο μέγιστο βαθμό, χωρίς περιορισμό σε throughput και logs per day προτείνουμε να αλλάξει σε:Η προσφερόμενη αδειοδότηση της πλατφόρμας SIEM να γίνει για XXX αριθμό συστημάτων χωρίς περιορισμό σε EPS, throughput ή GB per day.ΕΡΩΤΗΣΗΣτην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης	**ΌΧΙ**	Ως προς το 1ο σκέλος, τα στοιχεία θα συλλεχθούν από τον ανάδοχο με την υποστήριξη της ΑΑΔΕ κατά τη μελέτη εφαρμογής.Ως προς το 2ο σκέλος, η διατύπωση παρέμεινε ως έχει καθώς η αλλαγή που προτείνεται μπορεί να περιορίσει τον ανταγωνισμό.

				Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 1 αναφέρεται:Η πλατφόρμα SIEM πρέπει να υποστηρίζει αυτόματες ενέργειες «Security Orchestration, Automation and Response» (SOAR). Οι λειτουργίες ασφαλείας και η ικανότητα αυτοματισμού πρέπει να συνδυάζουν ευφυή αυτοματισμό και ενορχήστρωση καθώς επίσης και δυνατότητες συλλογικής έρευνας. Πρέπει να επιτρέπουν στους αναλυτές SOC να έχουν συνεπείς και τεκμηριωμένες δυνατότητες διερεύνησης απειλών και threat hunting αξιοποιώντας ενέργειες SOAR που βασίζονται σε playbooks, πληροφορίες αυτόματης ανίχνευσης και machine learning για ταχύτερη ανάλυση και καλύτερη απόδοση της υπηρεσίας SOC.Για να μπορέσει ο φορέας να αξιοποιήσει στο μέγιστο δυνατό βαθμό τόσο τις δυνατότητες της πλατφόρμας SIEM όσο και της λύσης SOAR προτείνουμε η συγκεκριμένη προδιαγραφή να αλλαχθεί σε:Η πλατφόρμα SIEM πρέπει να υποστηρίζει και να ενσωματώνεται με αυτόματες ενέργειες πλατφόρμας «Security Orchestration, Automation and Response» (SOAR) του ίδιου κατασκευαστή. Οι λειτουργίες ασφαλείας και η ικανότητα		

				αυτοματισμού πρέπει να συνδυάζουν ευφυή αυτοματισμό και ενορχήστρωση καθώς επίσης και δυνατότητες συλλογικής έρευνας. Πρέπει να επιτρέπουν στους αναλυτές SOC να έχουν συνεπείς και τεκμηριωμένες δυνατότητες διερεύνησης απειλών και threat hunting αξιοποιώντας ενέργειες SOAR που βασίζονται σε playbooks, πληροφορίες αυτόματης ανίχνευσης και machine learning για ταχύτερη ανάλυση και καλύτερη απόδοση της υπηρεσίας SOC.		

31	**Βασιλική Δεμέστιχα**	-	Παρατήρηση	ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Το λογισμικό θα πρέπει να μπορεί να χρησιμοποιεί ποικιλία μεθόδων συσχέτισης (correlation) logs όπως π.χ.: (α) Rule-Based (β) Statistical-based, (γ) Historical-based, (δ) Human-based. Να αναφερθούν οι δυνατότητες. Καθώς δεν είναι ξεκάθαρο ποια η διαφορά των τεσσάρων κατηγοριών ενώ προωθείται λύση συγκεκριμένου κατασκευαστή, προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Να υποστηρίζει την αποθήκευση των ακατέργαστων δεδομένων (raw data) σε εξωτερικό αποθηκευτικό χώρο. Επίσης είναι απαραίτητο τα raw data να συμπιέζονται και στη συνέχεια να κρυπτογραφούνται και να υπογράφονται ψηφιακά (digitally signed) με κλειδί κρυπτογράφησης γνωστό μόνο στον οργανισμό.	**ΝΑΙ**	Η απαίτηση "Το λογισμικό θα πρέπει να μπορεί να χρησιμοποιεί ποικιλία μεθόδων συσχέτισης (correlation) logs όπως π.χ.: (α) Rule-Based (β) Statistical-based, (γ) Historical-based, (δ) Human-based. Να αναφερθούν οι δυνατότητες." της παραγράφου 8.2.6.3 διατηρήθηκε ως έχει καθώς οι όροι που χρησιμοποιούνται είναι διαδεδομένοι και δεν περιορίζει τους συμμετέχοντες. Η απαίτηση "Να υποστηρίζει την αποθήκευση των ακατέργαστων δεδομένων (raw data) σε εξωτερικό αποθηκευτικό χώρο. Επίσης είναι απαραίτητο τα raw data να συμπιέζονται και στη συνέχεια να κρυπτογραφούνται και να υπογράφονται ψηφιακά (digitally signed) με κλειδί κρυπτογράφησης γνωστό μόνο στον οργανισμό." της παραγράφου 8.2.6.3 προστέθηκε ως επιθυμητή. Η απαίτηση "Εφαρμογή για

				Η συγκεκριμένη περιγραφή προωθεί λύση συγκεκριμένου κατασκευαστή και προτείνουμε να αλλαχθεί ως εξής: Να υποστηρίζει την αποθήκευση των ακατέργαστων δεδομένων (raw data). ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Εφαρμογή για κινητές συσκευές Android™ και Apple™ με δυνατότητα ειδοποίησης μέσω Push notifications για alerts και incidents. Καθώς για λόγους ασφαλείας η πλειοψηφία των κατασκευαστών λύσεων SIEM αποφεύγει τη χρήση mobile apps, προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Είναι επιθυμητό να παρέχει τη δική της λύση Endpoint Detection & Response (EDR) με τα παρακάτω χαρακτηριστικά:		κινητές συσκευές Android™ και Apple™ με δυνατότητα ειδοποίησης μέσω Push notifications για alerts και incidents." της παραγράφου 8.2.6.3, προστέθηκε ως επιθυμητή. Η απαίτηση "Είναι επιθυμητό να παρέχει τη δική της λύση Endpoint Detection & Response (EDR)" της παραγράφου 8.2.6.3, διατηρήθηκε.

				ο Πλήρης διαχείριση μέσω της πλατφόρμας ο File Integrity Monitoring ο Application Control ο Yara Rules ο Watchdog Η συγκεκριμένη απαίτηση δεν εμπίπτει στις δυνατότητες της SIEM πλατφόρμας και προτείνουμε να αφαιρεθεί.		

32	**Βασιλική Δεμέστιχα**	demestic@gr.ibm.com	Παρατήρηση	ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Εϊναι επιθυμητό το λογισμικό να παρέχει λύση για ανίχνευση κακόβουλων επιθέσεων και threat-actors που έχουν καταφέρει να αποκτήσουν πρόσβαση στο σύστημα (Deception technology). Η λύση θα δίνει τη δυνατότητα εγκατάστασης ψευδών αρχείων και υπολογιστών εντός δικτύου με σκοπό την παραπλάνηση και έγκαιρη ανίχνευση των threat-actors. Όλα τα δεδομένα να μπορούν να παρουσιαστούν και σε οπτική απεικόνιση για εύκολη κατανόηση από τον χειριστή του ιστορικού σε περίπτωση συμβάντος. Η συγκεκριμένη απαίτηση δεν εμπίπτει στις δυνατότητες της SIEM πλατφόρμας και προτείνουμε να αφαιρεθεί. ΕΡΩΤΗΣΗ Στην παράγραφο 8.2.6.3, στις Λειτουργικές απαιτήσεις λογισμικού διαχείρισης Περιστατικών ασφαλείας (SIEM) στην προδιαγραφή 3 αναφέρεται: Δυνατότητα για σύνδεση με Active	**ΟΧΙ**	Η απαίτηση "Εϊναι επιθυμητό το λογισμικό να παρέχει λύση για ανίχνευση κακόβουλων επιθέσεων και threat-actors που έχουν καταφέρει να αποκτήσουν πρόσβαση στο σύστημα (Deception technology)" της παραγράφου 8.2.6.3, παρέμεινε. Η απαίτηση "Δυνατότητα για σύνδεση με Active Directory με σκοπό την επιθεώρηση των λογαριασμών των χρηστών" της παραγράφου 8.2.6.3, παρέμεινε.

				Directory με σκοπό την επιθεώρηση των λογαριασμών των χρηστών για: ο Ανενεργούς χρήστες (rogue accounts) ο Nested groups ο Επιτυχείς και ανεπιτυχείς προσπάθειες πρόσβασης ο Ληγμένους κωδικούς ο Soon-to-expire passwords Να αναφερθούν οι δυνατότητες Η διασύνδεση με το Active Directory γίνεται ώστε οι χρήστες που υπάρχουν στο Active Directory, να αποκτήσουν πρόσβαση στο SIEM με τον ίδιο λογαριασμό. Επιπλέον, σε αυτή την απαίτηση θα βοηθήσουν οι λύσεις PAM και IAM που έχουν προδιαγραφεί σε άλλα κεφάλαια και για το λόγο αυτό προτείνουμε να αφαιρεθεί από τη συγκεκριμένη ενότητα.		
33	**Petros Vasilikos - COSMOS BUSINESS SYSTEMS AEBE**	vassilikosp@cbs.gr	Πίνακας 4: Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (Privileged Access Management)	Στην σελίδα 89 του κειμένου διαβούλευσης και συγκεκριμένα στον Πίνακα 4: Λειτουργικές απαιτήσεις λογισμικού διαχείρισης των προσβάσεων των Διαχειριστών (Privileged Access Management) , περιγράφεται μια λυση Ασφαλούς Διαχείρισης των Προσβάσεων των Προνομιακών Λογαριασμών (Privileged Access Management – PAM) η οποια θα πρπει να επιτρέπει στον φορέα: • να διαμοιράσει με ασφαλή τρόπο την απαιτούμενη πρόσβαση στους	**ΝΑΙ**	Ως προς τα δυο πρώτα σημεία/παρατηρήσεις του οικονομικού φορέα, δεν ενσωματώθηκαν καθώς καλύπτονται από υφιστάμενες αναφορές. Ως προς την απαίτηση για προσθήκη δυνατότητας παράκαμψης του συστήματος (Break the Glass), ενσωματώθηκε για περιορισμένο αριθμό

				εξωτερικούς της συνεργάτες, • να εφαρμόσει ενιαίο και ασφαλή τρόπο διαχείρισης των κωδικών πρόσβασης των προνομιακών λογαριασμών, • να μειώσει την επιφάνεια επίθεσης, • να καταγράψει και να παρακολουθήσει τις συνεδρίες των εξωτερικών συνεργατών , τόσο απολογιστικά όσο και real time. • να παρακολουθεί με ενεργητικό αλλά και παθητικό τρόπο τον κύκλο ζωής των προνομιακών λογαριασμών, • να επιτρέψει την ασφαλή είσοδο με πολυπαραγοντική ταυτοποίηση και να αποθηκεύσει και διαμοιράσει με ασφαλή τρόπο κλειδιά ασφαλείας και πιστοποιητικά. Καθώς λύσεις τέτοιας κατηγορίας είναι πολύ επικίνδυνο να προκαλέσουν αδυναμία πρόσβασης στην υποδομή του οργανισμού , σε περίπτωση δυσλειτουργίας του λογισμικού ή της υποδομής που φιλοξενεί το λογισμικό , κρίνεται επιβεβλημένο η λύση που τελικά θα επιλεγεί να παρέχει την δυνατότητα : 1. Να υποστηρίζει την δυνατότητα λειτουργίας σε redundancy 2. Να παρέχει την δυνατότητα ,		χρηστών (ενδεικτικά μέγιστος 3).

				μεταξύ άλλων , και άμεσης τηλεφωνικής εξυπηρέτησης , από τον κατασκευαστή του λογισμικού , 24x7x365 . 3. Να παρέχει με αποδεδειγμένα ασφαλή τρόπο δυνατότητα παράκαμψης του συστήματος (Break the Glass).		
34	**Netcompany - Intrasoft S.A.**	maria.orfanou@netcompany.com	8. ΠΑΡΑΡΤΗΜΑ Ι – ΑΝΑΛΥΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΦΥΣΙΚΟΥ ΚΑΙ ΟΙΚΟΝΟΜΙΚΟΥ ΑΝΤΙΚΕΙΜΕΝΟΥ ΤΗΣ ΣΥΜΒΑΣΗΣ – ΑΠΑΙΤΗΣΕΙΣ - ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ	Παρακαλούμε πολύ όπως δοθεί παράταση ως προς την καταληκτική ημερομηνία υποβολής σχολίων/ παρατηρήσεων για 2 εβδομάδες δεδομένου της πολυπλοκότητας του έργου και των τεχνικών απαιτήσεων	**ΟΧΙ**	Το αίτημα έχει ικανοποιηθεί
35	**Παναγιώτης Πανταζής**	smyrniosc@unisystems.gr	Παρατήρηση 1Στην §2.2.6 «Τεχνική και επαγγελματική ικανότητα» στο σημείο 2 γίνεται η εξής αναφορά:• «Τουλάχιστον ένα (1) έργο υλοποίησης IAM (Identity & Access Right Management), ένα (1) έργο υλοποίησης PAM (Privileged Access Management) και ένα (1) έργο υλοποίησης SIEM (Security Information and	Θεωρούμε ότι η αναφορά για την αντίστοιχη δραστηριότητα με την ΑΑΔΕ είναι πολύ περιοριστική λαμβάνοντας υπόψη το μέγεθος του έργου και προτείνουμε την προσθήκη του όρου δημόσιος φορέας αντίστοιχου μεγέθους με την ΑΑΔΕ με βάση τον αριθμό των χρηστών / συσκευών που θα εξυπηρετηθούν	**ΟΧΙ**	Η απαίτηση έχει απαντηθεί στο σχόλιο 14.

			Event Management) σε φορέα αντίστοιχης δραστηριότητας με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα).».			
36	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 2 Στην §2.2.6 «Τεχνική και επαγγελματική ικανότητα» στο σημείο Γ. αναφέρονται τα ακόλουθα: • Να εξυπηρετεί/παρακολουθεί τουλάχιστον πενήντα (50) πελάτες στο Κέντρο Λειτουργιών Ασφάλειας για υπηρεσίες Managed Security Services (MSS) ή/και Managed Detection and Respond (MDR). • Να απασχολεί τουλάχιστον είκοσι πέντε (25) αναλυτές L1 ως L4.	Θεωρούμε ότι η ποσότητα των πελατών δεν προσφέρει κάτι σε οργανισμούς όπως η ΑΑΔΕ, και είναι αντίθετη από την ικανότητα που ζητείται. Προτείνουμε να προτιμηθούν στοιχεία, όπως το είδος των πελατών / οργανισμών που εξυπηρετούνται ή το μέγεθος των πελατών / οργανισμών που εξυπηρετούνται. Επίσης, το πλήθος και level αναλυτών δεν είναι μετρήσιμο ως προς την ποιότητα και τα SLA του SOC. Προτείνουμε να προτιμηθούν μετρήσιμα στοιχεία SLA όπως το MTTR (Mean Time To Recovery).	**ΟΧΙ**	Η παρατήρηση δεν ενσωματώθηκε καθώς η προδιαγραφή προστέθηκε για να διασφαλίσει ότι το προσφερόμενο SOC θα αντιστοιχεί στο μέγεθος της ΑΑΔΕ την εμπειρία του υποψηφίου αναδόχου. Επιπλέον, αφορά την επιχειρησιακή ικανότητα του SOC και δεν σχετίζεται με το SLA.

37	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 3 Στην §2.2.6 «Τεχνική και επαγγελματική ικανότητα» για τα τρία (3) Μέλη ομάδας έργου Κέντρου επιχειρήσεων ασφάλειας (SOC) απαιτούνται οι εξής πιστοποιήσεις: • Certified Information Security Manager (CISM) ή ισοδύναμη από αναγνωρισμένους Φορείς Πιστοποίησης. • Certified Information Systems Auditor (CISA) ή ισοδύναμη από αναγνωρισμένους Φορείς Πιστοποίησης. • Certified Ethical Hacker (CEH) ή ισοδύναμη από αναγνωρισμένους Φορείς Πιστοποίησης. • Certified Information Systems Security Professional (CISSP) ή ισοδύναμη από αναγνωρισμένους Φορείς Πιστοποίησης.	Θεωρούμε ότι οι πιστοποιήσεις CISA και CEH δεν έχουν εφαρμογή στα καθήκοντα του συγκεκριμένου ρόλου και προτείνουμε να αφαιρεθούν.	**ΝΑΙ**	Η πρόταση για απαλοιφή της απαίτησης για πιστοποίηση CISA ενσωματώθηκε στη διακήρυξη καθώς καλύπτεται εν μέρει από τις απαιτήσεις για άλλες πιστοποιήσεις. Η πρόταση για απαλοιφη της απαίτησης για πιστοποίηση CEH δε γίνεται δεκτή καθώς η πιστοποίηση αυτή εισάγει στην ομάδα SOC καλύτερη κατανόηση των τεχνικών επιθέσεων και συμβάλει στην αποκάλυψη ευπαθειών και στην αντιμετώπιση απειλών.
38	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 4 Στην §2.2.6 «Τεχνική και επαγγελματική ικανότητα» για το Σύμβουλο Κέντρου επιχειρήσεων ασφάλειας	Θεωρούμε ότι η συγκεκριμένη πιστοποίηση δεν έχει εφαρμογή στα καθήκοντα του συγκεκριμένου ρόλου και προτείνουμε να αφαιρεθεί.	**ΟΧΙ**	Η πρόταση για απαλοιφή της απαίτησης για πιστοποίηση OSCP παρέμεινε καθώς πιστοποιεί την ικανότητα "επιθετικής" αποκάλυψης, ανάλυσης και διαχείρισης

			(SOC) απαιτείται η πιστοποίηση «Offensive Security Certified Professional (OSCP) ή ισοδύναμη από αναγνωρισμένους Φορείς Πιστοποίησης.»			των ευπαθειών σε συστήματα και θεωρείται σημαντική πιστοποίηση και για αναλυτές SOC, στο πλαίσιο των τάσεων για "επιθετική" άμυνα
39	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 5 Στην §8.2.6.1 «Λογισμικό Identity and Access Rights Management (IAM) για τον έλεγχο της πρόσβασης χρηστών στα πληροφοριακά συστήματα» τα σημεία 22 και 23 του Πίνακα 3 επαναλαμβάνουν κείμενο που περιλαμβάνεται στο σημείο 18 του ίδιου πίνακα.	Προτείνουμε να αφαιρεθούν.	**ΝΑΙ**	Διορθώθηκε το κείμενο με διαγραφή των σημείων 22 και 23
40	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 6 Στην §8.2.12 «Υπηρεσίες Πιλοτικής και Ένταξης σε Παραγωγική Λειτουργία» γίνονται οι εξής αναφορές: • «Την υποστήριξη χρηστών από απόσταση αλλά και με φυσική παρουσία στελεχών του Αναδόχου (συλλογή παρατηρήσεων από τους χρήστες, υποστήριξη στο χειρισμό και λειτουργία των λογισμικών, κλπ.).»	Παρακαλούμε να επιβεβαιώσετε την κατανόησή μας ότι η παροχή των παραπάνω υπηρεσιών θα λάβουν χώρα στην έδρα της Γ.Δ.ΗΛΕ.Δ. στην Αθήνα.	**ΌΧΙ**	Επιβεβαιώνεται η κατανόηση του οικ. Φορέα ότι η παροχή υπηρεσιών θα λάβει χώρα εντός Αττικής

			και • «Την παροχή τεχνικής υποστήριξης on-site προκειμένου να μεταφερθεί η απαραίτητη τεχνογνωσία χρήσης των λογισμικών στα στελέχη του φορέα.»			
41	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 7 Στην §8.2.12 «Υπηρεσίες Πιλοτικής και Ένταξης σε Παραγωγική Λειτουργία» γίνεται η εξής αναφορά: • «Αναλυτικότερα, για την επίτευξη αυτής της υποχρέωσης, ο Ανάδοχος οφείλει να προτείνει μεθοδολογία ελέγχου και να συνεργαστεί με τον φορέα κατά την εφαρμογή της. Η μεθοδολογία που θα προταθεί από τον Ανάδοχο πρέπει να περιλαμβάνει, κατ' ελάχιστον, i) τον προγραμματισμό των ελέγχων, ii) τον προσδιορισμό του περιεχομένου των ελέγχων, iii) την υλοποίηση των ελέγχων από τον ανάδοχο με την επίβλεψη της ΑΑΔΕ, και iv) την τεκμηρίωση των	Παρακαλούμε επιβεβαιώστε την κατανόησή μας ότι η παραπάνω υποχρέωση αφορά τον ανάδοχο και θα συμπεριληφθεί στη Μελέτη Εφαρμογής που θα εκπονηθεί κατά την Φάση Β του Έργου.	**ΝΑΙ**	Επιβεβαιώνεται η κατανόηση του οικ. Φορέα. Για να μην υπάρχει ασάφεια ως προς το πότε θα παραδοθεί η μεθοδολογία για τα UAT, έγινε προσαρμογή στο κείμενο όσον αφορά το παραδοτέο (Π.Β.6) σε συνάρτηση με το σημείο 5 της 8.2.11.

			αποτελεσμάτων του ελέγχου.»			
42	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 8 Στην §8.2.13 «Υπηρεσίες Εκπαίδευσης και μεταφοράς τεχνογνωσίας» γίνεται η εξής αναφορά: • Η προσφερόμενη εκπαίδευση θα γίνει από πιστοποιημένους συνεργάτες-εκπαιδευτές του κατασκευαστή του λογισμικού στην Αθήνα, είτε με φυσική παρουσία είτε με σύγχρονη εξ αποστάσεως εκπαίδευση. Στην περίπτωση φυσικής παρουσίας, τα σεμινάρια εκπαίδευσης θα λάβουν χώρα υποχρεωτικά σε αναγνωρισμένα και πιστοποιημένα από τον κατασκευαστή του προσφερόμενου λογισμικού εκπαιδευτικά	Λαμβάνοντας υπόψη ότι τα προσφερόμενα συστήματα / λογισμικά είναι 4, θεωρούμε ότι η αναφορά της πιστοποίησης του εκπαιδευτικού κέντρου από τον κατασκευαστή / τους κατασκευαστές είναι περιοριστική και προτείνουμε την αφαίρεσή της.	**ΝΑΙ**	Απαλήφθηκε η απαίτηση για "πιστοποιημένα από τον κατασκευαστή του προσφερόμενου λογισμικού εκπαιδευτικά κέντρα " και παρέμεινε η αναφορά μόνο ως πιστοποιημένα εκπαιδευτικά κέντρα.

			κέντρα στην Αθήνα. Σε περίπτωση παροχής σύγχρονης εξ αποστάσεως εκπαίδευσης, ο Ανάδοχος θα παρέχει την απαιτούμενη υποδομή και περιβάλλον εκπαίδευσης			
43	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 9Στην §8.2.14 «Υπηρεσίες Security Operation Center (SOC)» γίνεται η εξής αναφορά:• Η διασύνδεση μεταξύ των συστημάτων του Security Operations Center (SOC) του Αναδόχου όπως ticketing system, κ.λπ. και του λογισμικού Security Incident and Event Management (SIEM), θα υλοποιείται μέσω μηχανισμών ισχυρής κρυπτογράφησης και αυθεντικοποίησης και πάνω από dedicated φυσική υποδομή (routers, leased lines, site-to-site ipsec vpn). Ο Ανάδοχος θα πρέπει να περιγράψει	Παρακαλούμε επιβεβαιώστε την κατανόησή μας ότι η παραπάνω υποχρέωση αφορά τον ανάδοχο και θα συμπεριληφθεί στη Μελέτη Εφαρμογής που θα εκπονηθεί κατά την Φάση Β του Έργου.Μπορεί να προστεθεί η πρόβλεψη στον πίνακα 7 και η απάντηση στο σχόλιο να είναι ότι ναι μεν η αναλυτική περιγραφή να είναι στη μελέτη.	**ΝΑΙ**	Προστέθηκε στον πίνακα 7 σημείο 2 του κεφαλαίου 8.2.7.1 "Ο Ανάδοχος θα πρέπει να περιγράψει τα δομικά χαρακτηριστικά της προτεινόμενης αρχιτεκτονικής διασύνδεσης και ολοκλήρωσης."Η οριστική αναλυτική περιγραφή των δομικών συστατικών θα πραγματοποιηθεί στη μελέτη εφαρμογής. Παράλληλα, για τους σκοπούς της αξιολόγησης οι υποψήφιοι ανάδοχοι θα πρέπει να παρουσιάσουν τα εν λόγω δομικά χαρακτηριστικά και στην τεχνική τους προσφορά, με τον βαθμό ανάλυσης που κρίνουν ότι επαρκεί για την αξιολόγηση.

			αναλυτικά τα δομικά χαρακτηριστικά της προτεινόμενης αρχιτεκτονικής διασύνδεσης και ολοκλήρωσης.			
44	UNISYSTEMS	smyrniosc@unisystems.gr	Παρατήρηση 10 Στον πίνακα με το ενδεικτικό χρονοδιάγραμμα του έργου (σελίδα 119), στην §8.3.1.4 «Υπηρεσίες SOC» και στην §8.3.2 «Συγκεντρωτικός Πίνακας Παραδοτέων» αναφέρεται ότι ο μήνας έναρξης της Φάσης Δ είναι ο Μ10. Στα υπόλοιπα σημεία του κειμένου της Διακήρυξης αναφέρεται ότι οι Υπηρεσίες SOC εκκινούν μαζί με την Φάση ΣΤ «Πιλοτική & Ένταξη σε Παραγωγική» ήτοι τον Μ11.	0	**ΝΑΙ**	Διορθώθηκε το κείμενο σε όλα τα σημεία ώστε να φαίνεται ότι η Φάση Δ εκκινείται τον μήνα 11.

45	NEUROSOFT	m.xylogiannopoulos@neurosoft.gr	Στην παράγραφο Β.4.Α. Για την απόδειξη της τεχνικής ικανότητας της παραγράφου 2.2.6.Α. οι οικονομικοί φορείς προσκομίζουν: πίνακα συναφών έργων που υλοποίησαν επιτυχώς κατά τα πέντε (5) τελευταία έτη, σύμφωνα με το ακόλουθο υπόδειγμα:	Προτείνουμε: 1. την αντικατάσταση της Κολώνας Διάρκεια έργου από – έως με ολοκληρωμένα ή εν' εξελίξει έργα, μιας και αναφερόμαστε σε έργα Υπηρεσιών (SOC) . 2. την αντικατάσταση της Κολώνας που αναφέρετε ο Πελάτης με Τομέας Δραστηριότητας (π.χ ενέργεια, μεταφορές, υγεία κοκ), μιας και αναφερόμαστε σε έργα Ασφάλειας Δεδομένων με σημαντικές κρίσιμες και ευαίσθητες πληροφορίες. 3. την διαγραφή της Κολώνας ΣΤΟΙΧΕΙΟ ΤΕΚΜΗΡΙΩΣΗΣ (τύπος & ημ/νία), μιας και αναφερόμαστε σε έργα Ασφάλειας Δεδομένων με σημαντικές κρίσιμες και ευαίσθητες πληροφορίες. Ως Στοιχείο Τεκμηρίωσης και στην περίπτωση που ο Πελάτης είναι Δημόσιος Φορέας, προτείνουμε να υποβάλλεται Δήλωση του Υποψήφιου Οικονομικού Φορέα όπου θα δεσμεύετε για την ορθότητα και εγκυρότητα των πληροφοριών που δηλώνει. Σε περίπτωση ανάθεσης του Έργου να πιστοποιείται η εγκυρότητα της υποβληθείσας Δήλωσης.	**ΝΑΙ**	Ως προς την 1η παρατήρηση, προστέθηκε υποσημείωση ότι αναφερόμαστε σε εν εξελίξει έργα που έχουν ξεκινήσει τουλάχιστον προ διετίας. Ως προς τα σημεία 2 και 3, οι προτάσεις του οικονομικού φορέα ενσωματώθηκαν στο κείμενο καθώς οι ανάγκες εμπιστευτικότητας αναμένεται να φέρουν σε δυσχέρεια στους υποψήφιους.

46	NEUROSOFT	m.xylogiannopoulos@neurosoft.gr	Στην Παράγραφο 8.2.14 Υπηρεσίες Security Operation Center (SOC), αναφέρεται Πιο συγκεκριμένα η προσφερόμενη υπηρεσία, θα πρέπει να παρέχει τις ακόλουθες λειτουργίες και χαρακτηριστικά: 17. Ειδικό πλαίσιο SOC II Type 2 εσωτερικού ελέγχου κυβερνοασφάλειας θα εφαρμόζεται στις εγκαταστάσεις του SOC του Ανάδοχου.	Προτείνουμε η συγκεκριμένη προδιαγραφή να τροποποιηθεί ώστε ο Υποψήφιος Ανάδοχος να είναι πιστοποιημένος ή να βρίσκεται σε διαδικασία πιστοποίησης κατά SOC II Type II με συγκεκριμένο χρονοδιάγραμμα.	**ΟΧΙ**	Η πρόταση του οικονομικού φορέα δεν ενσωματώθηκε καθώς εκτιμάται ότι θα περιορίσει τον ανταγωνισμό
47	NEUROSOFT	m.xylogiannopoulos@neurosoft.gr	Στην Παράγραφο 8.2.6.3 Λογισμικό Διαχείρισης Περιστατικών Ασφαλείας (SIEM) - Ειδικές απαιτήσεις, αναφέρεται: «Εφαρμογή για κινητές συσκευές Android™ και Apple™ με δυνατότητα ειδοποίησης μέσω Push notifications για alerts και incidents.»	Προτείνουμε η συγκεκριμένη προδιαγραφή να αφαιρεθεί ή τροποποιηθεί σε «επιθυμητή» καθότι αναφέρεται σε τεχνολογική λύση συγκεκριμένου/ων κατασκευαστή/ών.	**ΝΑΙ**	Η απαίτηση έχει απαντηθεί στο σχόλιο 31

48	Microsoft	andreasbotas@microsoft.com	8.2.6.3 - SIEM	1) Deception Technology Πιστεύουμε ότι η συγκεκριμένη απαίτηση δεν είναι μέρος μιας πλατφόρμας SIEM και προτείνουμε την απαλοιφή της 2) Εφαρμογή για κινητές συσκευές Η συγκεκριμένη απαίτηση προτείνουμε να αφαιρεθεί καθώς οι περισσότεροι leaders της αγοράς SIEM σύμφωνα με την Gartner δεν παρέχουν αυτή την δυνατότητα. 3) EDR, Yara Rules Η χρήση Yara Rules παραπέμπει σε συγκεκριμένους κατασκευαστές EDR και προτείνουμε να τροποποιηθεί προσθέτοντας και άλλα εργαλεία ευρέσεως και σύνταξης ερωτημάτων (όπως KQL) ή να αφαιρεθεί. Παράλληλα προτείνουμε τον εμπλουτισμό των προδιαγραφών ώστε να συμπεριληφθούν δυνατότητες διασύνδεσης για ingestion πληροφοριών από υπηρεσίες τρίτων καθώς και SaaS λύσεων όπως το Microsoft Office 365 και Microsoft Entra ID (Azure Active Directory). 4) Προτείνουμε να εμπλουτιστεί η	**ΝΑΙ**	Για το σημείο 1, η προδιαγραφή 3 "Εϊναι επιθυμητό το λογισμικό να παρέχει λύση για ανίχνευση κακόβουλων επιθέσεων και threat-actors που έχουν καταφέρει να αποκτήσουν πρόσβαση στο σύστημα (Deception technology)" της παραγράφου 8.2.6.3 παρέμεινε ως έχει καθώς εκτιμάται ότι είναι ζωτικής σημασίας για τους αναλυτές του SOC αφού θα επιτρέψει την πρόωρη ανίχνευση τυχόν κακόβουλων που κρύβονται εντός του οργανισμού καθώς επίσης και τυχόν προσπάθειας llateral movement. Οι αναλυτές μπορούν σε πραγματικό χρόνο να ενημερωθούν για την ενεργοποίηση συναγερμού από τη λύση έτσι ώστε να ενεργήσουν ανάλογα. Για το σημείο 2, η προδιαγραφή για κινητές συσκευες έγινε επιθυμητή. Για το σημείο 3 που αφορά την προδιαγραφή για EDR και Yara Rules, η προδιαγραφή είναι έτσι κι αλλιώς

				διαστασιολόγηση με βάση τον εκτιμώμενο ημερήσιο όγκο δεδομένων/logs ο οποίος μπορεί να προκύψει κατόπιν ανάλυσης των πηγών που θα συνδεθούν πχ. Users, Endpoint Devices , Servers, Emails. Σημειώνεται πως το Microsoft Sentinel προσφέρει οικονομίες κλίμακας, συνεργειών και μείωσης κόστους καθώς ποικιλία πηγών δεδομένων που προέρχονται από το Microsoft Azure και το Microsoft 365 μπορούν να ληφθούν (ingestion) χωρίς οικονομική επιβάρυνση. 5) Σημειώνεται πως στα συμβασιοποιημένα έργα, «G-Cloud Next Generation» με κωδικό ΟΠΣ 5073641, καθώς και «Παροχή Νεφο -Υπολογιστικών Υποδομών και υπηρεσιών (Cloud Services)» με κωδικό ΟΠΣ ΤΑ 5166485, σύμβαση 2197, προδιαγράφεται και διατίθενται τόσο «Υπηρεσία διαχείρισης πληροφοριών συμβάντων ασφαλείας (Security Information Event Management – SIEM) καθώς και «υπηρεσία αυτοματοποιημένης διαχείρισης περιστατικών ασφάλειας (Security Orchestration Automated Response - SOAR)», εντός των προσφερόμενων cloud services του G-Cloud της ΓΓΠΣΨΔ προς χρήση		επιθυμητή. Προστέθηκε ως επιθυμητό στην απαίτηση 3 του τμήματος "ειδικές απαιτήσεις" του πίνακα η εξής αναφορά "Είναι επιθυμητό το λογισμικό να παρέχει δυνατότητες διασύνδεσης για ingestion πληροφοριών από υπηρεσίες τρίτων καθώς και SaaS λύσεων. Να αναφερθούν οι δυνατότητες." Ως προς το σημείο 4, τα στοιχεία που αφορούν τον εκτιμώμενο ημερήσιο όγκο δεδομένων/Logs δεν είναι εφικτό να παρασχεθούν. Ως προς το σημείο 5, το αντικείμενο των έργων που παραθέτει ο οικονομικός φορέας δεν θα καλύψει τις ανάγκες της ΑΑΔΕ αλλά μόνο του Υπουργείου Ψηφιακής Διακυβέρνησης.

				και αξιοποίηση από τους κυβερνητικούς φορείς. Επομένως παρέχεται η δυνατότητα για μέγιστη αξιοποίηση υπαρχόντων κρατικών έργων και με συνεπακόλουθα οικονομικά οφέλη.		
49	Microsoft	andreasbotas@microsoft.com	Α.8	Η πλειοψηφία των σύγχρονων λύσεων λογισμικού, πρωτίστως λύσεων Software As A Service, προσφέρεται με συνδρομητικό εμπορικό μοντέλο, το οποίο περιλαμβάνει αναβαθμίσεις, ενημερώσεις, και φιλοξενία της λύσης για τα SaaS. Θεωρούμε ότι η επιβράβευση προτάσεων για λογισμικά απεριόριστης χρήσης δε συνάδει με τις σύγχρονες πρακτικές	**ΟΧΙ**	Η απαίτηση έχει ήδη απαντηθεί στο σχόλιο 2, δεν περιγράφεται η προμήθεια λύσεων SaaS λόγω της εγκατάστασης των λογισμικών στο g-cloud.

				της αγοράς και ενδεχομένως να οδηγήσει στην επιλογή παλαιότερων και υποδεέστερων λύσεων ασφάλειας για την Ανεξάρτητη Αρχή.		
50	Microsoft	andreasbotas@microsoft.com	Κεφ 8.2.4 Λογισμικά ασφάλειας και Άδειες Χρήσης	SIEM, συσκευές = 250 Όλες οι ηγετικές λύσεις SIEM τιμολογούνται με βάση είτε τον αριθμό των EPS ή τον αριθμό του όγκου των ημερήσιων logs (σε GB/day). Επομένως θα ήταν ιδανική περαιτέρω ανάλυση των απαιτήσεων με τον εκτιμώμενο αναμενόμενο όγκο logs και τον ακριβή τύπο των υπό διασύνδεση συσκευών. -IAM, λογαριασμοί = 13700 -PAM, χρήστες = 400 Παρακαλούμε όπως διευκρινίσετε τον αριθμό εσωτερικών (χρηστών εντός του ιδίου Active Directory) και εξωτερικών χρηστών καθώς η κοστολόγηση των εξωτερικών χρηστών στο Entra ID (Azure Active Directory) ξεκινάει πάνω από τους 50.000 μοναδικούς χρήστες τον μήνα καθιστώντας την ιδιαίτερα επωφελή για τον οργανισμό.	**ΟΧΙ**	Διεκρινίζεται ότι δεν είναι εφικτό να παρασχεθούν τα ζητούμενα στοιχεία τα οποία αναμένεται να συλλεχθούν από τον ανάδοχο με την υποστήριξη της ΑΑΔΕ κατά τη Μελέτη Εφαρμογής. Επιπλέον, διευκρινίζεται ότι το σύνολο των χρηστών που αναφέρονται στη διακήρυξη είναι εσωτερικοί.

51	Microsoft	andreasbotas@microsoft.com	8.2.6.1 Λογισμικό IAM	5. 13.700 λογαριασμούς.Παρακαλούμε όπως διευκρινίσετε τον αριθμό εσωτερικών και εξωτερικών χρηστών καθώς το Microsoft Entra ID (Azure Active Directory) διαθέτει διακριτή τιμολογιακή πολιτική για εσωτερικούς και εξωτερικούς χρήστες.3. Το λογισμικό θα εγκατασταθεί σε υποδομή η οποία θα παραχωρηθεί από την Αναθέτουσα Αρχή.Προτείνουμε τη διεύρυνση της προδιαγραφής, ώστε να μην αποκλείονται λύσεις Software As A Service, οι οποίες διαθέτουν ποικιλία πλεονεκτημάτων έναντι της παραδοσιακής τοπικής εγκατάστασης.6. Οι προσφερόμενες άδειες χρήσης λογισμικού της πλατφόρμας IAM θα επιτρέπουν στον Φορέα εάν το επιθυμεί να μεταφέρει και να λειτουργήσει την πλατφόρμα IAM σε υποδομές Public Cloud.Αντίστοιχα ζητούμε την τροποποίηση της συγκεκριμένης προδιαγραφής καθώς η παροχή οποιασδήποτε υπολογιστικής υποδομής ως πλατφόρμα εγκατάστασης περιορίζει κατά πολύ τις διαθέσιμες επιλογές του οργανισμού απορρίπτοντας τις κορυφαίες λύσεις της αγοράς οι οποίες παρέχονται σαν Software as	**ΌΧΙ**	Οι προτάσεις του οικονομικού φορέα δεν έγιναν αποδεκτές. Συγκεκριμένα διευκρινίζεται ότι 1. Το σύνολο των χρηστών είναι εσωτερικοί χρήστες2. Το λογισμικό θα εγκατασταθεί στην υποδομή g-cloud. 3. Το λογισμικό θα εγκατασταθεί στην υποδομή g-cloud. 4. Η απαίτηση για αναφορά σε leaders σε report της Gartner μπορεί να είναι περιοριστική

				a Service. Επίσης θεωρούμε σημαντικό για την Αρχή, η προσφερόμενη λύση να είναι αναγνωρισμένη απο 3ους αναλυτές όπως η Gartner. Αξίζει να σημειωθεί ότι η Gartner δημοσιεύει κάθε χρόνο το “Magic Quadrant for Access Management” το οποίο αξιολογεί τέτοιες λύσεις . Προκειμένου ο οργανισμός να εξασφαλίσει την προμήθεια μιας αναγνωρισμένης λύσης να προστεθεί η αναφορά της λύσης στους Leaders του παραπάνω report.		
52	Neurosoft	m.xylogiannopoulos@neurosoft.gr	Παρατήρηση	2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24)Στην παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24) αναφέρεται: «Τουλάχιστον ένα (1) έργο υλοποίησης IAM (Identity & Access Right Management), ένα (1) έργο υλοποίησης PAM (Privileged Access Management) και ένα (1) έργο υλοποίησης SIEM (Security Information and Event Management) σε φορέα αντίστοιχης δραστηριότητας με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα).»Παρακαλούμε πολύ να απαληφθεί η φράση «σε φορέα	**ΝΑΙ**	Η απαίτηση θα ενσωματωθεί μερικώς με διαγραφή της αναφοράς σε αντίστοιχης δραστηριότητας φορέα" όπως αναφέρεται στο σχόλιο 14.

				αντίστοιχης δραστηριότητας με την ΑΑΔΕ (π.χ. ελεγκτικό φορέα, χρηματοπιστωτικό ίδρυμα» μιας και περιορίζει τους συμμετέχοντες		
53	Neurosoft	m.xylogiannopoulos@neurosoft.gr	Παρατήρηση	Στην Παράγραφο 2.2.6 Τεχνική και επαγγελματική ικανότητα (σελ. 24) αναφέρετε: «Τα έργα θα πρέπει να έχουν συνολικό προϋπολογισμό ίσου ή μεγαλύτερο του 50% του προϋπολογισμού του έργου μη συμπεριλαμβανομένου Φ.Π.Α και του δικαιώματος προαίρεσης. Σε κάθε ένα από τα ανωτέρω έργα θα πρέπει να τεκμηριώνεται και η παροχή υπηρεσιών εγκατάστασης, παραμετροποίησης και εκπαίδευσης.» Παρακαλούμε πολύ να αντικατασταθεί σε: «Τα έργα θα πρέπει να έχουν συνολικό προϋπολογισμό ίσου ή μεγαλύτερο του 30% του προϋπολογισμού του έργου»	**ΝΑΙ**	Έχει απαντηθεί στο σχόλιο 15