ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XL..
Ερωτήματα που έχουν τεθεί μέχρι τις 3/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ

Α/Α	Σημείο από RFP	Ερωτήματα /Διευκρινήσεις που ζητήθηκαν από προμηθευτές	Απαντήσεις ΚΕΔΙΠΕΣ
1	**Dark Web Monitoring** Παράρτημα 2 / 2.7 Siem Threat Intelligence Operatoins / Τεχνική Προδιαγραφή 3: Optional Dark web, Deep web, clear net monitoring for potential attacks to the organization Παράρτημα 2 / 3 Managed SOC Requirements / Τεχνική Προδιαγραφή 11: Vendor must monitor dark web for KEDIPES related exposure.	*Το Dark Web Monitoring αναφέρεται σε δύο διαφορετικές τεχνικές προδιαγραφές, στη μία ως προαιρετικό (Optional) και στην άλλη ως υποχρεωτικό.* *Παρακαλούμε όπως διευκρινίσετε ποια από τις δύο προδιαγραφές υπερισχύει, δηλαδή εάν η απαίτηση για Dark Web Monitoring θεωρείται προαιρετική ή υποχρεωτική.*	Η απαίτηση για Dark Web Monitoring είναι υποχρεωτική.
2	**Flexible Authentication** Παράρτημα 2 / 2.2 Log Sources and Monitoring / Τεχνική Προδιαγραφή 7: Flexible user authentication — local, external via Microsoft AD and OpenLDAP, Cloud SSO/SAML via Okta, Duo, RADIUS	*Η απαίτηση αυτή αφορά κυρίως δυνατότητες ολοκλήρωσης με συστήματα διαχείρισης ταυτότητας και πρόσβασης (IAM / SSO) και όχι τις βασικές λειτουργίες ενός SIEM (συλλογή, ανάλυση, συσχέτιση και διαχείριση συμβάντων ασφαλείας).* *Η χρήση τοπικών λογαριασμών στην πλατφόρμα, με ελεγχόμενη διαδικασία απόδοσης και άμεσης ανάκλησης πρόσβασης μπορεί να διασφαλιστέι μέσω:* *• Πολυπαραγοντικής αυθεντικοποίησης (Multi-Factor Authentication - MFA)* *• Περιορισμού πρόσβασης βάσει γεωγραφικής τοποθεσίας (Geo-location based access control)* *Οι ανωτέρω μηχανισμοί καλύπτουν πλήρως τις απαιτήσεις ασφαλούς πρόσβασης των χρηστών.*	Η υποστήριξη των αναφερόμενων μηχανισμών δεν συνεπάγεται υποχρεωτική χρήση όλων αυτών από την ΚΕΔΙΠΕΣ

		Η αυθεντικοποίηση μέσω εξωτερικών καταλόγων χρηστών (Microsoft AD, OpenLDAP) απαιτεί σύνδεση του εσωτερικού δικτύου / Collector με πλατφόρμα που φιλοξενείται εκτός αυτού, είτε με άνοιγμα εισερχόμενης πρόσβασης είτε με πρόσθετα ενδιάμεσα συστήματα (AD FS, Entra Connect), με αποτέλεσμα μεγαλύτερη επιφάνεια επίθεσης, πολυπλοκότητα και κόστος συντήρησης. *Με τοπικούς λογαριασμούς σε συνδυασμό με MFA και γεωγραφικό περιορισμό, το επίπεδο ασφάλειας παραμένει ισοδύναμο ή υψηλότερο, χωρίς καμία έκθεση της εσωτερικής υποδομής.* *Ως εκ τούτου, παρακαλούμε όπως η απαίτηση για υποστήριξη συγκεκριμένων εξωτερικών μηχανισμών αυθεντικοποίησης (Microsoft AD, OpenLDAP, Okta, Duo, RADIUS κ.λπ.) αφαιρεθεί ή θεωρηθεί προαιρετική.*	
3	**In-scope Assets**	*In-scope Assets* *No in-scope assets have been included in the tender documents.*	Ο κατάλογος των Assets θα παραδίνεται στην ενδιαφερόμενη εταιρεία κατόπιν αιτήματος στο tendersdepartment@kedipes.com.cy
4	**Service Delivery/Clarifications** Παράρτημα 2 / 1 General Requirements / Τεχνική Προδιαγραφή 3: The platform should be hosted in a data center or cloud located within the EU with ISO/IEC 27001 certification. The service provider shall maintain ISO/IEC 27001 certification while the underlying cloud and platform services shall have SOC 2 Type II certification.	*Παρακαλούμε να διευκρινιστεί ότι η απαίτηση πιστοποίησης SOC 2 αφορά τον πάροχο των υπηρεσιών (MSSP/SOC Service Provider) και τις διαδικασίες, τους ελέγχους και τις υπηρεσίες που παρέχει προς τον οργανισμό και όχι την προσφερόμενη πλατφόρμα ή τα επιμέρους προϊόντα λογισμικού που αποτελούν μέρος της λύσης.*	The platform shall be hosted in a data center or cloud infrastructure located within the European Union. That hosting facility shall hold a current ISO/IEC 27001 certification. The Service Provider (the entity providing the service) shall itself hold a current ISO/IEC 27001 certification for its information security management system and shall provide a current SOC 2 Type II attestation report covering the security operations services delivered under this contract.

5	**Gartner Leaders** Παράρτημα 2 / 2.1 Siem Platform Features / Τεχνική Προδιαγραφή 18: The proposed SIEM platform must be actively maintained, have a clear product roadmap, and remain supported throughout the contract period (i.e., no end-of-life) This solution should have been positioned as a leader by any of the following Technology Analysts over the last 2 years (IDC, Gartner, Forester)	*Η αναγνώριση ενός SIEM κατασκευαστή από διεθνώς αναγνωρισμένους αναλυτικούς οίκους, όπως οι Gartner, Forrester ή IDC, αποτελεί σημαντική ένδειξη τεχνολογικής ωριμότητας, καινοτομίας και παρουσίας στην αγορά.* *Ωστόσο, η απαίτηση ο κατασκευαστής να έχει καταταχθεί αποκλειστικά στην κατηγορία "Leaders" κατά τα τελευταία δύο (2) έτη ενδέχεται να περιορίσει αδικαιολόγητα τον ανταγωνισμό, καθώς οι σχετικές αξιολογήσεις περιλαμβάνουν και άλλες κατηγορίες (π.χ. Visionaries, Challengers, Niche Players) οι οποίες αναγνωρίζουν λύσεις με αποδεδειγμένη τεχνική επάρκεια και υψηλό επίπεδο καινοτομίας.* *Παρακαλούμε όπως αφαιρεθεί η απαίτηση "Leader" με αντικατάσταση ως απαίτηση αναγνώρισης ή συμπερίληψης του κατασκευαστή στις σχετικές αξιολογήσεις των εν λόγω αναλυτικών οίκων τουλάχιστον μία φορά τα τελευταία τρία χρόνια, ώστε η αξιολόγηση να εστιάζει πρωτίστως στις τεχνικές δυνατότητες, τη συνεχή υποστήριξη, το product roadmap και την πλήρη κάλυψη των απαιτήσεων του έργου. Παράλληλα εισηγούμαστε όπως η συγκεκριμένη απαίτηση αφαιρεθεί στην περίπτωση που η πλατφόρμα SIEM αλλά και οι υπηρεσίες SOC παρέχονται από τον κατασκευαστή.*	Η απαίτηση αναγνώρισης από Gartner, Forrester ή IDC **δεν** θα αποτελεί υποχρεωτικό κριτήριο αποκλεισμού, αλλά θα θεωρείται πρόσθετο τεχνικό πλεονέκτημα κατά την τεχνική αξιολόγηση. Στην περίπτωση όπου η πλατφόρμα SIEM και οι υπηρεσίες SOC παρέχονται από τον κατασκευαστή, η απουσία τέτοιας αναγνώρισης **δεν** θα επηρεάζει την αποδοχή της προσφοράς, νοουμένου ότι καλύπτονται πλήρως οι τεχνικές και λειτουργικές απαιτήσεις του διαγωνισμού.
6	**Attack Simulation Services** Παράρτημα 2 / 2.7 SIEM Threat Intelligence Operations / Τεχνική Προδιαγραφή 7:	*Παρακαλούμε όπως επανεξεταστεί η συμπερίληψη των δραστηριοτήτων adversary emulation και purple*	Η απαίτηση αφορά ενέργειες επιβεβαίωσης της ορθής λειτουργίας του συστήματος.

	MSSP should provide attack simulation and security validation services to assess the effectiveness of security controls, SIEM detections, SOC processes, incident response capabilities and monitoring effectiveness. The service should support activities such as adversary emulation, purple teaming, detection validation, use-case validation and control effectiveness assessments.	*teaming στην παρούσα απαίτηση και αφαιρεθούν από το αντικείμενο του διαγωνισμού.* *Οι συγκεκριμένες δραστηριότητες αποτελούν εξειδικευμένες υπηρεσίες αξιολόγησης ασφάλειας, οι οποίες συνήθως εντάσσονται στο πλαίσιο υπηρεσιών Red Teaming, Purple Teaming ή Security Assessment Services και δεν αποτελούν τυπικές ή βασικές λειτουργίες μιας υπηρεσίας SOC.* *Προτείνεται η απαίτηση να περιοριστεί σε δραστηριότητες που σχετίζονται άμεσα με τη λειτουργία του SOC και την αποτελεσματικότητα των μηχανισμών ανίχνευσης και απόκρισης, όπως:* • *Detection validation* • *Use-case validation* • *SIEM correlation rule validation* • *Monitoring effectiveness assessment* • *Incident response process validation* *ώστε το αντικείμενο της απαίτησης να παραμείνει ευθυγραμμισμένο με το πεδίο παροχής υπηρεσιών SOC/MDR και να αποφευχθεί η εισαγωγή εξειδικευμένων υπηρεσιών offensive security που αποτελούν ξεχωριστό αντικείμενο προμήθειας και αξιολόγησης*	Διευκρινίζεται ότι οι υπηρεσίες security validation θα πρέπει να περιλαμβάνουν κατ' ελάχιστον: • Detection validation • Use-case validation • SIEM correlation rule validation • Monitoring effectiveness assessment • Incident response process validation προς αξιολόγηση της αποτελεσματικότητας των μηχανισμών παρακολούθησης και απόκρισης. Δυνατότητες όπως adversary emulation & purple teaming θα θεωρηθούν πρόσθετο τεχνικό πλεονέκτημα και θα αξιολογηθούν θετικά κατά την τεχνική αξιολόγηση.
7	**User Identity, Location & Account Information** Παράρτημα 2 / 2.1 Siem Platform Features / Τεχνική Προδιαγραφή 4: User Identity, Location & Account Information The solution should provide user web activity monitoring (Website categories,	*Η παρακολούθηση και κατηγοριοποίηση διαδικτυακής χρήσης (URL categorization, web content filtering) δεν αποτελεί τυπική ή βασική λειτουργία ενός SIEM. Πρόκειται για χαρακτηριστικό εξειδικευμένων λύσεων Secure Web Gateway / Web Proxy, όχι μιας λύσης συλλογής και συσχέτισης συμβάντων ασφαλείας. Ένα SIEM μπορεί να αξιοποιήσει τα logs που παράγουν τέτοιες λύσεις, όχι να αντικαταστήσει τη λειτουργία τους. Παρακαλούμε όπως η απαίτηση αφαιρεθεί από τις προδιαγραφές SIEM και αντικατασταθεί με*	Διευκρινίζεται ότι **δεν** απαιτείται η παροχή εγγενούς λειτουργικότητας Web Filtering ή Secure Web Gateway από την πλατφόρμα SIEM. Η απαίτηση αφορά τη δυνατότητα παρακολούθησης, συσχέτισης και αναφοράς δραστηριοτήτων χρηστών στο διαδίκτυο μέσω εγγενών δυνατοτήτων ή/και μέσω ενσωμάτωσης και αξιοποίησης δεδομένων

	accessed files with suspicious extensions). User policy violations like Inappropriate website access, unauthorized access etc.	*απαίτηση υποστήριξης τηλεμετρίας (log ingestion) από υφιστάμενες ή τρίτες λύσεις Web Proxy / Secure Web Gateway.*	καταγραφής από τρίτες λύσεις ασφαλείας (Secure Web Gateways, Web Proxies ή αντίστοιχες πλατφόρμες).
8	**Log Retention/ Data Storage** Παράρτημα 2 / 2.6 SIEM Platform Infrastructure / Τεχνική Προδιαγραφή 4: Indicate data retention capabilities of the platform. Minimum should be 12 months in hot storage. Παράρτημα 2 / 2.6 SIEM Platform Infrastructure / Τεχνική Προδιαγραφή 5: The proposed solution must support a minimum log retention for a period of three (3) months. Παράρτημα 2 / 2.2 Log Sources and Monitoring / Τεχνική Προδιαγραφή 10: Logs should be stored the same storage (hot storage, fully searchable) for a period of at least 6 months.	*Οι προδιαγραφές αναφέρουν τρεις διαφορετικές περιόδους για την αποθήκευση/αναζήτηση δεδομένων σε hot storage: 12 μήνες (Data Availability & Storage), 3 μήνες live search, και 6 μήνες fully searchable. Παρακαλούμε να διευκρινίσετε ποια πολιτική ισχύει.*	Η προδιαγραφή αλλάζει ως εξής: 6 μήνες συνολική διατήρηση δεδομένων (retention period), πλήρως διαθέσιμη για ανάκτηση και διερευνητικούς σκοπούς μέσω της SIEM πλατφόρμας. 4 εβδομάδες διατήρηση δεδομένων με δυνατότητα άμεσης και πλήρους αναζήτησης (live search).
9	**Attack Surface Monitoring and Dark Web Monitoring**	*Οι απαιτήσεις Attack Surface Monitoring (§2.7, Προδιαγραφές 1 και 3) και Dark Web Monitoring (§3.1, Προδιαγραφή 3) αποτελούν συμπληρωματικές*	Η απαίτηση παραμένει ως έχει.

ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XDR
Ερωτήματα που έχουν τεθεί μέχρι τις 3/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ

	Παράρτημα 2 / 2.7 SIEM Threat Intelligence Integrations / Τεχνική Προδιαγραφή 1: MSSP should be able to optionally provide external attack surface monitoring. (eg., Monitoring network perimeter for exposed services, unusual changes, software versions) (Optional) Παράρτημα 2 / 2.7 SIEM Threat Intelligence Integrations / Τεχνική Προδιαγραφή 3: Threat Intelligence team, if required must be in a position to provide Operational Intelligence. Operational Intelligence should include but not be limited to (Optional): Παράρτημα 2 / 3.1 SOC Service Coverage and Operating Model / Τεχνική Προδιαγραφή 3: Vendor must monitor dark web for KEDIPES related exposure.	*διαστάσεις της ίδιας λειτουργίας Cyber Threat Exposure Management.* *Προτείνουμε την ενιαία μεταχείρισή τους, με αναβάθμιση καί των δύο απαιτήσεων σε υποχρεωτικές, ώστε να διασφαλίζεται πλήρης και συγκρίσιμη κάλυψη της εξωτερικής έκθεσης του Οργανισμού.*	Η ΚΕΔΙΠΕΣ καθορίζει τις υποχρεωτικές και προαιρετικές απαιτήσεις σύμφωνα με τις επιχειρησιακές και λειτουργικές ανάγκες. Η παροχή επιπρόσθετων δυνατοτήτων Cyber Threat Exposure Management συμπεριλαμβανομένων Attack Surface Monitoring & Dark Web Monitoring, πέρα των υποχρεωτικών απαιτήσεων, θα αξιολογηθούν θετικά κατά την τεχνική αξιολόγηση.
10	SIEM Licensing Volume	*Παρακαλούμε όπως μας δοθεί ο ακριβής ημερήσιος όγκος καταγραφών (GB/day) ώστε να καταστεί η ορθή διαστασιολόγηση και κοστολόγηση της προσφερόμενης υπηρεσίας.*	40 GB / day
11	EDR	*Παρακαλούμε όπως δοθεί ο ακριβής αριθμός χρηστών (workstations and servers) για σκοπούς σωστής αδειοδότησης κατά την διάρκεια των πέντε χρόνων που αναφέρεται στην οικονομική προσφορά.*	Ο κατάλογος των Assets θα παραδίνεται στην ενδιαφερόμενη εταιρεία κατόπιν αιτήματος στο tendersdepartment@kedipes.com.cy
12	EDR/XDR Table 4.5 Investigation and Remediation, Requirement 16 and 17	*Η δυνατότητα SOAR Playbooks (Off-the-shelf και custom) αποτελεί λειτουργία της πλατφόρμας SIEM/SOC και όχι χαρακτηριστικό του EDR/XDR agent. Η απαίτηση αυτή καλύπτεται ήδη στους πίνακες SIEM*	Η απαίτηση παραμένει ως έχει. Αναγνωρίζεται ότι οι δυνατότητες SOAR playbooks μπορούν να παρέχονται είτε μέσω της πλατφόρμας

		(SOAR and Security Automation, Στοιχείο 2· SIEM Technology Integration, Στοιχείο 4) και SOC (SOC Tools, Integration and Continuous Improvement, Στοιχείο 4). Προτείνουμε την αφαίρεσή της από τον πίνακα EDR/XDR για αποφυγή διπλής καταγραφής της ίδιας απαίτησης.	SIEM/SOAR είτε μέσω της πλατφόρμας EDR/XDR. Η εν λόγω απαίτηση αποσκοπεί στην επιβεβαίωση της διαθεσιμότητας των σχετικών δυνατοτήτων αυτοματοποίησης και απόκρισης ανεξαρτήτως της αρχιτεκτονικής υλοποίησης του κατασκευαστή.
13	Section 2.1 Automated Infrastructure Discovery & Application Discovery Engine	*For SIEM to operate as expected, it has a built in CMDB and Automated Discovery Feature that is utilised as the "Source of Truth" for various operations. We request the following alteration of the requirement to: "SIEM should support integration Asset Management or operate its internal CMDB solution*	The requirement is changed to: *"SIEM should support integration Asset Management or operate its internal CMDB solution".*
14	Section 2.1 SIEM Platform Features Requirement 20 (Data Masking):	*The requirement conflicts with Section 2.4 SIEM Deployment and Support and raw log storage and archiving. Every vendor has a different methodology of performing obfuscation/masking of data depending on their deployment model and supported architecture. If obfuscation/masking is performed at the collector, then for cloud-based infrastructure it is not possible to revert the obfuscation/masking since the data reside in the cloud infrastructure not the collector.*	The requirement is changed to: *The solution must provide granular data masking/obfuscation capabilities allowing the customer to define specific data fields for obfuscation. Data de-obfuscation must support an approval process that is catalogued and recorded. The solution must guarantee that no sensitive information is de-obfuscated without a build in approval process to the request.*
15	Section 2.2 Log Source and Monitoring Requirement 2 AI Capabilities	*The requirement as presented is limiting the utilisation of AI Frontier models. Each vendor has a different approach in implementing AI features on their platform and the requirement as set forth*	The requirement is changed to: AI utilisation is allowed given that one of the two following conditions are met. Condition 1, the AI

		is limiting the utilisation of resources that could benefit the customer and excludes platforms from competing in the RFP.	processing must be hosted within the SIEM provider's private data center infrastructure. Condition 2, an external AI model can be utilised when information send for inference and processing are anonymised
16	Section 2.4 SIEM Deployment and Support Requirement 1 Deployment and Support	*The requirement specifies that the solution should integrate with KEDIPES's Asset Management Platform. This is applicable for certain vendors only.*	The requirement is modified to include the following: The solution should be integrated with KEDIPES's Asset Management Platform or provide a build in CMDB capabilities