

ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XDR

Ερωτήματα που έχουν τεθεί μέχρι τις 30/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ

A/A	Σημείο από RFP			Ερωτήματα /Διευκρινήσεις που ζητήθηκαν από προμηθευτές	Απαντήσεις ΚΕΔΙΠΕΣ
1	Ο πάροχος πρέπει να υποβάλει στοιχεία νομικής υπόστασης, εταιρικής εγγραφής, αδειοδοτημένων όπου εφαρμόζεται και δήλωση ότι δεν έχει υποστεί ουσιώδεις εποπτικές κυρώσεις, διοικητικά πρόστιμα ή περιοριστικά μέτρα τα τελευταία πέντε (5) έτη.	Υποχρεωτικό	1. Πιστοποιητικό Εγγραφής 2. Εταιρική Δομή 3. Δηλώσεις Κανονιστικής Συμμόρφωσης	In relation to requirement 3, Kindly pls clarify what does this entail. Our understanding is that a declaration confirming the below (definition of «Εταιρική Κανονιστική Συμμόρφωση» on the web) is sufficient, but kindly pls advise	Ο πάροχος θα πρέπει να υποβάλει υπογεγραμμένη δήλωση ότι κατά τα τελευταία πέντε (5) έτη δεν του έχουν επιβληθεί πρόστιμα, κυρώσεις ή άλλοι περιορισμοί από εποπτικές ή ρυθμιστικές αρχές. Σε περίπτωση που έχουν επιβληθεί κυρώσεις ή πρόστιμα κατά την τελευταία πενταετία, ο πάροχος θα πρέπει να τα γνωστοποιήσει περιγράφοντας τη φύση τους, το ύψος του προστίμου ή της κύρωσης και τα διορθωτικά μέτρα που λήφθηκαν για την αντιμετώπιση του ζητήματος.
2	QUESTION & ANSWERS until 8.9.2026 Clarification 3 Customer-Managed Keys (BYOK/CMK) με δυνατότητα ανάκλησης από την Αναθέτουσα Αρχή			<i>In multi-tenant environments the SOC Operator utilises CMKs for the management of the cloud infrastructure. The possibility for end-customers to revoke Certificates for multi-tenant infrastructure is not possible.</i> <i>We request the requirement to change as follows:</i> <i>"For Single-Tenant configuration the platform must utilise customer managed Keys with possibility of revocation of certificates from Contracting Authority. For multi-tenancy environments the SOC provider must utilise a Key Management</i>	The intent of this requirement is not the hosting model, but ensuring effective control over access to KEDIPES data. The suggested wording is therefore modified as follows: For Single-Tenant configuration the platform must utilise customer managed Keys with possibility of revocation of certificates from Contracting Authority. For multi-tenancy environments the SOC provider must utilise a Key Management Service (BYOK or CMK or KMS), or an equivalent key managed mechanisms that

ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XDR

Ερωτήματα που έχουν τεθεί μέχρι τις 30/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ

		Service (BYOK or CMK or KMS) that provides key rotation and revocation in case of security incidents from the SOC Operator".	provide key rotation and revocation, provided that KEDIPES retains an effective and auditable mechanism to revoke, suspend, or disable access to its data and encryption keys, and is not solely depended on the SOC provider or SOC Operator for exercising such control.
3	QUESTION & ANSWERS until 8.9.2026 Clarification 16 Δήλωση συνολικού μεγέθους ομάδας SOC και αναλογίας αναλυτών ανά εξυπηρετούμενο πελάτη, ως στοιχείο τεκμηρίωσης (βαθμολογούμενο, μη αποκλειστικό).	Διευκρινίζεται ότι η αναλογία αναλυτών ανά εξυπηρετούμενο πελάτη δεν θα πρέπει να αξιολογείται αυτοτελώς ως δείκτης επάρκειας ή ποιότητας της υπηρεσίας, καθώς υψηλότερη αναλογία πελατών ανά αναλυτή δύναται να προκύπτει από αυξημένο βαθμό αυτοματοποίησης, orchestration και βελτιστοποίησης της λειτουργίας του SOC. Ως εκ τούτου, προτείνεται η αναλογία αυτή να χρησιμοποιείται αποκλειστικά ως πληροφοριακό στοιχείο τεκμηρίωσης και να μην αποτελεί βαθμολογούμενο κριτήριο.	Το αίτημα δεν γίνεται αποδεκτό. Η δήλωση του συνολικού μεγέθους της ομάδας SOC και της αναλογίας αναλυτών ανά εξυπηρετούμενο πελάτη, παραμένει βαθμολογούμενο αλλά μη αποκλειστικό στοιχείο τεκμηρίωσης και δεν θα αξιολογηθεί αυτοτελώς.

ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XDR**Ερωτήματα που έχουν τεθεί μέχρι τις 30/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ**

4	QUESTION & ANSWERS until 8.9.2026 Clarification 16 Υποχρέωση προηγούμενης έγκρισης αντικατάστασης καίριων ρόλων.	<i>Σε περίπτωση αντικατάστασης, προτείνεται να απαιτείται η ενημέρωση της Αναθέτουσας Αρχής και η τεκμηρίωση ότι το νέο πρόσωπο διαθέτει ισοδύναμα ή ανώτερα προσόντα και εμπειρία, χωρίς να απαιτείται προηγούμενη έγκριση για αλλαγές στο ευρύτερο προσωπικό ή στη στελέχωση του SOC που δεν επηρεάζουν την εκπλήρωση των συμβατικών υποχρεώσεων.</i>	Συμφωνούμε.
5	Μεθοδολογία Αξιολόγησης Προσφορών	<i>Παρακαλούμε όπως διευκρινίσετε αναλυτικά τη μεθοδολογία αξιολόγησης και βαθμολόγησης των Προσφορών, περιλαμβανομένων των κριτηρίων, των συντελεστών βαρύτητας, του τρόπου υπολογισμού της τελικής βαθμολογίας και τυχόν ελάχιστων απαιτούμενων βαθμολογιών ανά κριτήριο ή/και συνολικά.</i>	Η μεθοδολογία θα καθοριστεί από τα άτομα της ad hoc τεχνικής επιτροπής αξιολόγησης.

ΔΙΑΓΩΝΙΣΜΟΣ 17/2026 – SIEM/SOC – EDR/XDR

Ερωτήματα που έχουν τεθεί μέχρι τις 30/9/2026 & Απαντήσεις της ΚΕΔΙΠΕΣ

6	3.1 SOC Service Coverage and Operating Model 3 Service Coverage The SOC service should provide L1, L2 and L3 analyst support with documented roles and responsibilities Και 3.2 SOC Roles and Responsibilities • Βιογραφικά και πιστοποιήσεις για συγκεκριμένους καίριους ρόλους: SOC Manager, Lead L3 Analyst / Threat Hunter, Incident Response Lead, Service Delivery Manager. και 1 L1 Analyst Role The SOC service should include L1 analysts responsible for alert monitoring, initial triage, validation, classification and ticket creation. 2 L2 Analyst Role The SOC service should include L2 analysts responsible for investigation, enrichment, correlation, incident analysis and escalation recommendations. 3 L3 Analyst Role The SOC service should include L3 analysts responsible for advanced analysis, threat hunting, complex incident support and detection improvement recommendations. 4 SOC Team Lead The SOC service must include a designated Team Lead / Service Delivery Manager responsible for oversight, quality control, SLA compliance monitoring, and serving as the primary escalation contact for KEDIPES leadership.	<i>The requirements regarding the SOC roles appear to differ between Sections 3.1 and 3.2. Section 3.1 requires L1, L2 and L3 analyst support, while Section 3.2 refers to the SOC Manager, Lead L3 Analyst / Threat Hunter, Incident Response Lead and Service Delivery Manager, and separately defines the roles of L1, L2, L3 Analysts and SOC Team Lead / Service Delivery Manager. Please clarify the exact SOC roles that are mandatory and identify for which roles CVs and certifications must be submitted with the Tender.</i> • <i>Is it acceptable that one person cover more than one of the required roles, particularly SOC Manager / Team Lead / Service Delivery Manager?</i>	Οι αναφορές στις ενότητες 3.1 και 3.2 είναι συμπληρωματικές. Οι L1, L2 και L3 περιγράφουν λειτουργικές βαθμίδες. Οι τέσσερις καίριοι ρόλοι καλύπτουν διακυβέρνηση και εξειδικευμένη ευθύνη. Ο ελεγχόμενος συνδυασμός ρόλων επιτρέπει ευελιξία, αλλά πρέπει να προστατεύει τον διαχωρισμό καθηκόντων, την αναπλήρωση και τη συνεχή λειτουργία. Σημειώνεται ότι είναι αποδεκτό ένα άτομο να καλύπτει περισσότερους ρόλους με την προϋπόθεση ότι δεν θα υπάρχει οποιαδήποτε δυσλειτουργία στους ρόλους και τα καθήκοντα του ατόμου.
---	--	--	---