STATO MAGGIORE DELLA DIFESA

UFFICIO GENERALE DEL CENTRO DI RESPONSABILITÀ AMMINISTRATIVA
AREA PROCUREMENT
UFFICIO CONTRATTI
Via XX Settembre n. 123/A - 00187 ROMA
C.F. 80248290589
PEC stamadifesa@postacert.difesa.it

Procedura ristretta mediante ricorso al Sistema Dinamico di Acquisizione della Pubblica Amministrazione per il potenziamento delle capacita cyber dedicate alla gestione delle identità digitali e alla sicurezza degli accessi all'intera info struttura ICT della Difesa (DIFENET)

APPALTO SPECIFICO N. 5827963
Elenco Chiarimenti

Aggiornato al 16/12/2025

N.	DOMANDA	RISPOSTA
1.	Si chiede di specificare il numero di utenti attivi e foreste presenti su Active Directory	Il numero di utenti attivi è 20.000 su una foresta.
2.	Si segnala che sul Capitolato Speciale d'appalto, all'art. 5, l'importo dell'appalto è € 348.840,00. Sulla piattaforma MEPA, invece, il valore dell'appalto è € 342.000,00	Si precisa che l'importo complessivo dell'appalto è pari a 342.000,00 IVA esente, come riportato in premessa della lettera di invito, in quanto l'importo riportato nel capitolato è comprensivo della quota da destinare agli incentivi per le funzioni tecniche ai sensi dell'art. 45 del D.Lgs. 36 del 2023.
3.	È tassativo che la soluzione venga installata in modalità on premises, o c'è la possibilità di poter proporre una soluzione di tipo SaaS?	È tassativo che la soluzione sia in modalità on premises.
4.	Si chiede di confermare che in relazione all'R3 agentless e scanless si riferisce alle postazioni di lavoro e non ai Domain Controller.	Il requisito R3 si riferisce sia alle postazioni di lavoro che ai domain controller.
5.	Si chiede di confermare in merito all'R4 che sia possibile fornire anche un sistema separato per ogni foresta per garantire la corretta segregazione.	La soluzione deve prevedere un'unica console con cui è possibile effettuare anche la segregazione per ogni foresta.
6.	Si chiede di confermare che sia possibile fornire più prodotti integrati dello stesso vendor per raggiungere gli obiettivi dell'Amministrazione, garantendo coerenza con la base d'asta.	La soluzione deve prevedere un'unica console per raggiungere gli obiettivi dell'amministrazione.
7.	Si chiede di indicare il conteggio totale degli user per individuare il numero di licenze da quotare.	Il numero totale di utenti è 20.000.
8.	Quante foreste Active Directory sono presenti? Quanti domini Active Directory sono presenti?	Il numero di foreste presenti è 1. Il numero di domini presenti è 1.

	Quante unità organizzative (OU) sono presenti in totale?	Sono presenti 800 UO.
	Quanti oggetti totali (utenti, gruppi, computer, ecc.) sono gestiti in Active Directory?	Sono gestiti 20.000 oggetti totali su una foresta su un dominio.
	Qual è la dimensione e la complessità del vostro ambiente Microsoft Entra ID (numero di utenti, gruppi, applicazioni integrate)?	Attualmente non esiste un ambiente Microsoft Entra ID.
	Quanti utenti totali (umani e di servizio) devono essere monitorati dalla soluzione?	Attualmente, 20.000 su una foresta su un dominio. In ottica futura, si potranno mettere in piedi più domini e la soluzione dovrà garantire la copertura di 2 domini.
	La nuova soluzione dovrà estendere il monitoraggio oltre Active Directory e Entra ID (es. endpoint, applicazioni cloud, server membri)?	Si, direttamente attraverso le sue funzionalità base oppure indirettamente attraverso l'integrazione con altre piattaforme di sicurezza.
	Qual è la tecnologia SIEM attualmente in uso (es. Splunk, QRadar, Microsoft Sentinel)?	Splunk e QRadar.
	Qual è la tecnologia EDR attualmente in uso (es. SentinelOne, CrowdStrike, Microsoft Defender for Endpoint)?	Trellix.
	Con quali altri sistemi di sicurezza (es. SOAR, PAM) la nuova soluzione dovrà integrarsi per consolidare gli alert, arricchire il contesto e automatizzare le risposte?	Vulnerability Management (VM), Extended Detection and Response (XDR), Cyber Asset Attack Surface Management (CAASM), IT Service Management (ITSM) nonché garantire standard aperti quali API RESTful e Syslog.
	Quali sono i requisiti per l'invio di dati e alert a questi sistemi (es. formato, frequenza, livello di dettaglio)?	• Formato dei dati e messaggi L'alert deve essere formattato utilizzando standard noti e parsabili. I formati più comuni sono JSON, CEF e LEEF. Ogni alert deve contenere un set minimo di campi per l'identificazione, l'investigazione e la risposta. Esempi di campi sono ID Unico dell'Evento, Timestamp, Gravità, Fonte, Indirizzo IP/Hostname del Target. Le entità

		principali (utenti, gruppi, dispositivi) devono utilizzare nomi e formati coerenti con quelli utilizzati nel resto dell'ecosistema di sicurezza (ad esempio username deve essere sempre nel formato SAMAccountName o UPN). • Frequenza La rilevazione degli eventi di attacco (inclusi Golden Ticket, Pass-the-Hash e modifiche di privilegi improvvise) deve avvenire in tempo reale (latenza ideale inferiore a 30 secondi). La rilevazione degli eventi di configurazioni errate/debolezze (inclusi password Never Expires, account inattivi o configurazioni errate AD) deve avvenire periodicamente (ad esempio ogni 24 ore o dopo ogni scansione completa di AD). Il meccanismo di invio deve prevedere l'utilizzo di metodi push (ad esempio l'invio diretto via Syslog o connessione API persistente) per gli eventi critici, evitando metodi pull lenti. • Livello di dettaglio L'alert deve includere il punteggio di rischio calcolato dalla soluzione (ad esempio un punteggio da 1 a 100) per permettere al SOAR o al SIEM di fornire la giusta priorità all'incidente. L'alert deve specificare la catena di attacco (kill chain) rilevata (ad esempio "Utente A può raggiungere il Gruppo B tramite la relazione di Trust C"). L'alert deve includere un campo che suggerisca la misura correttiva specifica (ad esempio "Rimuovere l'utente dal gruppo X", "Forzare il cambio password dell'account Y", ecc.). Infine, la soluzione deve specificare l'attore, cioè l'utente che ha effettuato l'azione o che è compromesso, e l'oggetto, cioè la risorsa compromessa o modificata.
	Esistono vincoli specifici sull'installazione di software (agenti) sui Domain Controller o altri server critici?	La soluzione non deve prevedere l'installazione di software (agenti) sui Domain Controller o su altri server critici.
	Il servizio di manutenzione del prodotto (es. aggiornamenti, patch, troubleshooting) deve essere erogato 24/7?	Si.

	La manutenzione della VM/Server su cui risiede la soluzione è a carico dell'appaltatore?	No, l'ambiente virtuale su cui risiederà la soluzione verrà messo a disposizione dal COR e manutenuto dal COR.
	Se sì, questo servizio deve essere erogato 24/7?	No.
	La compilazione del registro elettronico delle attività (logging) deve essere a carico dell'appaltatore?	Si.
	Quali normative o standard di compliance (es. GDPR, ISO 27001, NIS2) devono essere supportati e dimostrati attraverso questa soluzione?	La soluzione deve supportare e dimostrare le seguenti normative e standard di compliance: ISO 27001, NIST, CIS, GDPR, NIS2, PCI DSS, SOX.
9.	Stante quanto riportato nel capitolato in riferimento al requisito mandatorio numero 14: la soluzione proposta deve nativamente prevedere questa tipologia di utenza per agganciarsi ed integrarsi all'Active Directory in oggetto?	La soluzione proposta deve prevedere nativamente l'utilizzo di un account di servizio read-only senza privilegi elevati, che garantisce l'impossibilità di modificare qualsiasi oggetto nell'ambiente Active Directory. La soluzione non deve richiedere accessi privilegiati sui domini monitorati oltre ai privilegi assegnati a uno standard account utente di dominio. Ogni funzionalità della soluzione dovrà essere eseguita da account senza privilegi elevati.
	Per quanto riferito nel capitolato al requisito mandatorio numero 10: la soluzione deve nativamente includere informazioni associate al MITRE ATT&CK o sono sufficienti altre linee guida di mercato?	La soluzione deve fornire nativamente, out of the box, informazioni di sicurezza fruibili, tra cui mappature MITRE ATT&CK tassativamente, punteggio del rischio di identità e integrazioni con piattaforme SIEM/SOAR.
10.	Relativamente al requisito R16: specificare cosa si intenda esattamente per modifiche non autorizzate agli utenti, ai gruppi e alle configurazioni di sistema.	La soluzione proposta deve utilizzare un meccanismo di monitoraggio basato su event streaming e analisi comportamentale (UEBA) per identificare e notificare automaticamente le modifiche di privilegi, appartenenza a gruppi o hash di password che deviano dalla baseline operativa o violano le policy di governance, garantendo la copertura completa dell'infrastruttura Active Directory.
	Sono disponibili elenchi o criteri/configurazioni che definiscono quali	No, non sono disponibili.

	configurazioni siano da considerarsi autorizzate? Il Cliente utilizza check-list o procedure interne per classificare e distinguere le modifiche autorizzate da quelle non autorizzate?	 Si, vengono utilizzate procedure interne.
11.	- Dimensionamento Infrastruttura Active Directory (On-Premise) Riferimento: Anx II RTO Par. 6.1 (R2): In riferimento al requisito R2 "Garantire la copertura di 2 domini", al fine di dimensionare correttamente le licenze software (il cui costo è tipicamente basato sul numero di utenze gestite), si chiede cortesemente di indicare il numero complessivo approssimativo di utenze attive (Enabled Users) presenti nei 2 domini oggetto della fornitura.	Attualmente, viene utilizzata una foresta con un dominio con 20.000 utenti attivi. Tuttavia, in ottica futura di poter mettere in piedi più domini, la soluzione deve garantire la copertura di 2 domini.
	- Dimensionamento Infrastruttura Azure AD/Entra ID (Cloud) Riferimento: Anx II RTO Par. 6.1 (R5): In riferimento al requisito R5 "Supportare Azure AD", si chiede di specificare se l'infrastruttura prevede uno scenario di identità ibrida e quale sia il numero approssimativo di utenze Azure AD/Entra ID da monitorare.	Attualmente, non esiste ancora ma in ottica futura la soluzione dovrà prevedere anche la gestione della sicurezza delle identità digitali in questo tipo di scenario.
	- Requisiti Infrastruttura On-Premise e Virtualizzazione Riferimento: Anx II RTO Par. 6.1 (R12); Art. 12 Capitolato: In riferimento al requisito R12 "Essere nativamente on-premise", si chiede conferma che l'Amministrazione fornirà le risorse infrastrutturali (Server Fisici o Virtual Machine) necessarie per l'installazione della soluzione. In caso affermativo, si chiede di specificare l'ambiente di virtualizzazione in uso presso il COR (es. VMware vSphere, Microsoft Hyper-V).	La soluzione verrà installata su ambiente virtualizzato messo a disposizione dal COR sulla base delle specifiche tecniche richieste per l'installazione. La soluzione deve supportare le piattaforme di virtualizzazione VMware vSphere / ESXi, Microsoft Hyper-V e Citrix Hypervisor.
	- Integrazione SIEM/SOAR Riferimento: Anx II RTO Par. 6.1 (R19): In riferimento al requisito R19, si chiede cortesemente di confermare quali specifiche piattaforme SIEM e/o SOAR sono attualmente in uso presso il COR e saranno oggetto di integrazione,	Splunk e QRadar come SIEM/SOAR

	indicandone se possibile la versione software.	
	- Definizione Orario di Servizio (SLA) Riferimento: Anx I Cpt Art. 14: In riferimento alla tabella degli SLA (Art. 14), i tempi di intervento sono espressi in "ore lavorative" e "giorni lavorativi". Si chiede cortesemente di definire la fascia oraria di copertura del servizio (es. Lunedì-Venerdì, 08:00-18:00, escluse festività).	Lunedì-Venerdì 08:00-18:00 escluse le festività per i livelli L3/L4. H24/7 inclusi i festivi per i livelli L1/L2.
	- Personale Formatore (Vendor vs Partner Certificato) Riferimento: Anx II RTO Par. 6.2: In riferimento al Training on Job, si richiede che la formazione sia erogata da "istruttori qualificati, commissionati dall'azienda vendor". Si chiede conferma che tale requisito sia soddisfatto anche impiegando istruttori appartenenti a un Partner tecnologico (l'Offerente), purché ufficialmente certificati e autorizzati dal Vendor stesso per l'erogazione della formazione specialistica richiesta.	No, la formazione deve essere erogata solo da istruttori qualificati commissionati dall'azienda vendor.
	- Logistica Formazione Riferimento: Anx II RTO Par. 6.2; Art. 10 Capitolato: In riferimento al Corso specialistico on-site per 15 unità, si chiede conferma che la sede sarà il COR (Via Stresa 31/B, Roma) e se l'Amministrazione metterà a disposizione un'aula idonea attrezzata con videoproiettore e/o se ci saranno anche lezioni che potranno svolgersi da remoto	La sede del corso sarà il COR (Via Stresa 31/B, Roma) e il COR metterà a disposizione un'aula idonea attrezzata con videoproiettore. Il corso deve essere erogato in modalità on-site.