



Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

**Chiarimenti - Appalto estraneo Tender 4330 – rfq_6674 avente ad oggetto:
FORNITURA DI SERVIZI DI SECURITY OPERATION CENTER, SOC.**

Quesito 1:

Buongiorno, si richiede quanto segue:

In merito al Capitolato Tecnico relativo alla fornitura dei servizi SOC, si chiede cortesemente di specificare se la Stazione Appaltante prevede dei requisiti minimi di retention per i log e gli eventi di sicurezza raccolti e gestiti dal servizio SOC.

In particolare, si richiede di conoscere:

- il periodo minimo di conservazione dei log/eventi (es. 6 mesi, 12 mesi, 24 mesi o diverso);
- eventuali differenziazioni tra log di tipo operativo e log/eventi di sicurezza;
- eventuali richieste di modalità specifiche di archiviazione (es. cold storage, cifratura, replica geografica).

Risposta quesito 1:

La differenziazione deve tener conto della diversa natura dei log: per i log operativi deve essere prevista una retention di 6 mesi, mentre per i log ed eventi di sicurezza la conservazione minima richiesta è di 12 mesi. Le modalità di archiviazione restano trasparenti per la Stazione Appaltante; ciò che rileva è la garanzia che i dati rimangano accessibili e integri per l'intero periodo di conservazione stabilito.

Quesito 2:

Si chiede di chiarire il dimensionamento previsto per la raccolta dei log, includendo volumi medi giornalieri e le aspettative di crescita o espansione futura del sistema di monitoraggio.

Risposta quesito 2:

L'informazione non è al momento disponibile, un eventuale dimensionamento può essere calcolato empiricamente considerando gli EPS medi indicati.





Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

Quesito 3:

In riferimento alla risposta al quesito 2 Pag.8 dei chiarimenti (afferente alle attività di Incident Handling) avremmo necessità di avere delucidazioni relative al ruolo, della “struttura interna di cybersecurity” citata nello specifico:
-Ruoli e responsabilità all’interno del processo schematizzato al paragrafo 2.4.5 FLUSSO RILEVAMENTO E GESTIONE EVENTI DI SICUREZZA del capitolato tecnico e con particolare interesse al passaggio 7 della procedura;
-Ownership delle attività legate alle tecnologie di gestione degli endpoint (AV, XDR futuro,MDM,etc.);
-Copertura oraria della struttura di cybersecurity della committente (gestione degli Incident in H24).

Risposta quesito 3:

L’ownership delle tecnologie di gestione degli endpoint è interna alla struttura della committenza.

Per quanto riguarda la copertura oraria della struttura di cybersecurity della committenza verrà resa disponibile in fase di kick-off.

Quesito 4:

In riferimento al diagramma di flusso cap. 2.4.5 step 7 cosa si intende per eventuale intervento di contenimento autonomo del SOC, in particolare:
- Se le azioni di contenimento devono essere attuate attraverso una tecnologia di orchestrazione(SOAR);
- Se le azioni di contenimento possono essere, in alternativa, attuate in collaborazione con la struttura interna di cybersecurity.

Risposta quesito 4:

Il perimetro e l’autonomia delle eventuali azioni di contenimento saranno decisi e concordati con l’aggiudicatario in fase di kick-off; le modalità utilizzate, comprese eventuali tecnologie di orchestrazione, per le suddette operazioni sono scelte e proposte tecniche specifiche del concorrente e saranno valutate in fase di gara.





Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

Le azioni di contenimento fuori da tale perimetro saranno attuate dalla Struttura Appaltante con eventuale collaborazione, se necessario.

Quesito 5:

- 1) quali possono essere i target dei PT (Tipologia),
- 2) il numero di target che possono essere coinvolti in ogni singolo PT,
- 3) Il numero di PT richiesti.

Risposta quesito 5:

Risposte già fornite in merito nei chiarimenti precedentemente pubblicati.

Quesito 6:

Alla pagina 14, paragrafo 3.2.1, è riportata la richiesta: “Elenco e descrizione degli altri strumenti di sicurezza correlati (ad es. IDS/IPS, Threat Intelligence Platform, SOAR)”.

Si chiede alla Committente di chiarire se, in base ai criteri di valutazione (ad esempio criterio 3, P3 – 20 punti), verranno attribuiti punteggi aggiuntivi a chi proporrà uno o più strumenti di sicurezza correlati come indicato nel paragrafo 3.2.1

Risposta quesito 6:

Come descritto nel paragrafo “Criterio 3” (cap. 8) punteggio sarà assegnato in base alla qualità complessiva, alla completezza e all'adeguatezza della soluzione tecnologica offerta. La proposizione di strumenti a corredo del SIEM, se coerenti e integrati, verrà considerata un elemento che contribuisce positivamente alla completezza della soluzione.





Acque SpA
Sede Legale
Via Garigliano 1, 50053, Empoli
Sede Amministrativa
Via Bellatalla 1, 56121, Ospedaletto, Pisa
tel 050 3165611, www.acque.net
info@acque.net, info@pec.acquespa.it

Quesito 7:

Per poter procedere con maggior accuratezza al dimensionamento del SIEM oggetto della gara è possibile confermare il numero approssimativo di utenti? Vi è possibile condividere anche il numero di Domain Controller?

Risposta quesito 7:

Le informazioni di dettaglio saranno condivise in fase di kick-off con l'aggiudicatario; l'informazione nota e riportata nel capitolato è il numero medio di EPS è pari a 2000.

Quesito 8:

Siamo a chiedere se, in relazione alla offerta Tecnica (cap. 7.1 del Capitolato Tecnico), sia richiesto di allegare i CV e gli attestati delle certificazioni del team di lavoro. Inoltre, poiché gli attestati sono nominativi, si deduce che i CV debbano essere nominativi. Si chiede cortese conferma.

Risposta quesito 8:

I CV possono essere allegati in forma anonimizzata.

Data 12/09/2025

Il responsabile del contratto

Ing. Francesco Branchitta

