INDAGINE DI MERCATO
FORNITURA DEL SERVIZIO DI INFORMATION SECURITY OPERATIONS MANAGEMENT
UAGEC 1973

DESCRIZIONE DEL SERVIZIO

Il Servizio di "Information Security Operations Management" è finalizzato a fornire alla Direzione Sicurezza Informatica dell'Autorità un supporto specialistico operativo nella pianificazione, coordinamento ed esecuzione delle attività di sicurezza informatica, con l'obiettivo di garantire un adeguato livello di protezione delle risorse informative, dei sistemi e dell'infrastruttura tecnologica dell'Autorità.

Il Servizio dovrà contribuire, in coerenza con le politiche dell'Autorità, alla definizione, implementazione e miglioramento continuo delle misure di sicurezza, nonché al rafforzamento delle capacità di prevenzione, rilevazione e risposta agli incidenti di sicurezza informatica.

In particolare il fornitore dovrà garantire il supporto operativo nelle seguenti attività:

- definizione, aggiornamento e applicazione di policy e procedure di sicurezza;
- analisi degli eventi rilevanti ai fini della sicurezza informatica, inclusi quelli relativi ai sistemi di posta elettronica, con particolare riferimento alle segnalazioni degli utenti relative a possibili rischi connessi all'utilizzo della posta elettronica (es. phishing, allegati sospetti, tentativi di social engineering)**;**
- monitoraggio, analisi e gestione degli allarmi di sicurezza generati dai sistemi di protezione in uso presso l'Autorità, con particolare riferimento alla sicurezza degli endpoint e ai sistemi di protezione a livello DNS (Cisco Umbrella);
- gestione operativa delle piattaforme di cybersecurity awareness e simulazione di campagne di phishing, inclusa l'analisi dei risultati e la predisposizione di reportistica;
- assistenza agli utenti per problematiche inerenti alle piattaforme di cybersecurity awareness e agli altri sistemi gestiti dalla Direzione Sicurezza Informatica, inclusa la gestione delle richieste, il supporto operativo e il coordinamento con eventuali fornitori o strutture tecniche coinvolte**;**
- gestione operativa delle piattaforme di vulnerability assessment (Qualys Enterprise True Risk)**,** comprensiva della definizione di piani di remediation e della gestione del ciclo di vita delle vulnerabilità;
- monitoraggio, analisi e gestione degli Alert, dei bollettini e delle comunicazioni emesse dallo CSIRT Italia**,** nonché provenienti da ulteriori CERT e Information Sharing & Analysis Center (ISAC), con attività di correlazione, contestualizzazione e valutazione del potenziale impatto sugli asset dell'Autorità e conseguente attivazione delle azioni di mitigazione;
- installazione, configurazione e gestione di sistemi di monitoraggio (es. PRTG Network Monitor, Nagios), inclusa la definizione delle soglie di allarme, la configurazione delle sonde e l'integrazione con i sistemi di sicurezza;
- installazione e configurazione di componenti infrastrutturali, tra cui apparati di rete (router, switch, access point e altri dispositivi di networking), sistemi operativi e ambienti di virtualizzazione, nonché supporto alla loro gestione operativa in ottica di sicurezza;
- supporto alle attività di modellazione della rete e analisi delle interdipendenze tra servizi, inclusa la definizione e manutenzione di modelli di service dependency mapping finalizzati a migliorare le capacità di monitoraggio, analisi degli impatti e gestione degli incidenti;
- supporto alle attività di notifica degli incidenti di sicurezza in conformità alla normativa vigente (tra cui il D. Lgs. 138/2024 e la L. 90/2024);

- gestione dei processi di escalation verso le strutture interne ed esterne competenti, inclusi CSIRT-Italia e le autorità di polizia giudiziaria;
- supporto alle attività di tuning e ottimizzazione dei sistemi e dei servizi di rilevazione degli eventi di sicurezza.

Si sottolinea che le soluzioni e i sistemi menzionati (Qualys, Cisco Umbrella, PRTG Network Monitor, etc.) potranno essere oggetto di modifica nel corso dell'esecuzione del Contratto.

Il Servizio dovrà assicurare:

- il miglioramento continuo della capacità di prevenzione e gestione degli incidenti;
- la riduzione dei tempi di rilevazione e risposta agli eventi di sicurezza;
- un costante allineamento alle minacce emergenti e alle indicazioni degli organismi nazionali e internazionali;
- la produzione di reportistica periodica sulle attività svolte, sullo stato della sicurezza e sulle principali criticità rilevate.

Il Servizio dovrà essere svolto in modalità "A CONSUMO" e l'erogazione delle giornate di supporto specialistico, nonché l'ambito operativo di riferimento dello stesso, dovranno essere di volta in volta preventivamente concordati con la Direzione Sicurezza Informatica.

La decorrenza del Servizio è indicata presuntivamente alla data del 1° luglio 2026.

Il Contratto che verrà sottoscritto avrà una durata di 12 mesi con opzione di rinnovo di altri 12 mesi alle stesse condizioni tecnico-economiche, salvo quanto previsto dall'art. 60 del d.lgs. n. 36/2023 e s.m.i. e dall'Allegato II.2-bis.

Per lo svolgimento del Servizio si reputano congrue 230 giornate uomo annue di consulenza specialistica da erogare necessariamente in presenza, salvo diverse indicazioni della Direzione Sicurezza Informatica, per un valore annuo indicativo di 70.000 euro IVA esclusa.

Qualora dovesse verificarsi l'ipotesi per la quale, alla scadenza del termine contrattuale previsto in 12 mesi, avanzassero le preventivate "giornate uomo" potrà essere facoltà dell'Autorità di prorogare il termine contrattuale per il loro utilizzo fino alla data del 31 dicembre 2027.

Le singole giornate di intervento da erogare "A CONSUMO" potranno essere attivate, secondo necessità, dall'Autorità con apposita comunicazione tramite e-mail con un preavviso minimo di 16 ore.

Le attività dovranno essere erogate dal lunedì al sabato nell'ambito dell'orario 8.00-17.00.

Il personale che fornirà i servizi specialistici dovrà essere in possesso di una formazione professionale specialistica sui sistemi in uso sopra specificati, possedere certificazioni in materia di sicurezza informatica rilevanti per gli ambiti di attività sopra riportati e dovrà possedere adeguate competenze tecniche negli ambiti generici della sicurezza informatica, del networking e della gestione dei sistemi, nonché esperienza operativa in contesti analoghi. In aggiunta alle competenze tecniche, sono richieste proattività, orientamento al risultato, precisione e puntualità, motivazione e affidabilità, nonché adeguate capacità di comunicazione e collaborazione per un efficace coordinamento con le strutture interne ed esterne.

Saranno previste in contratto clausole volte a tutelare l'Autorità in merito alla riservatezza delle informazioni raccolte dall'impresa fornitrice nella fase esecutiva del Servizio.