وزارة التعليم العالي والبحث العلمي
ⵓⵖⵏⴻⵀⵍⵙⵙⵓⵙⴰⵙⵙⴻⵔⵜⴰⵙⵙⴰⵏⴻⵙⵙⵓⵓⵍ
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

مركز البحث في الإعلام العلمي والتقني
ⵓⵔⵔⵓ ⵍⵙⴰⵏⴻ ⵖⵜⵜ ⵜⵙⵏⵖⵜ ⵜⵙⵓⵍⵙⵜ ⴰ ⵜⵙⵜⵍⵔⵏⵙⵜ

Centre de Recherche sur l'Information Scientifique et Technique
Research Centre on Scientific and Technical Information

CAHIER DES CHARGES
RELATIF A LA SELECTION
D'UN PRESTATAIRE SPECIALISEE DANS L'INFOGÉRANCE EN CYBERSECURITE (AUDIT, SURVEILLANCE CONTINUE ET INTERVENTION EN CAS D'INCIDENT DE SECURITE)

مركز البحث في الإعلام العلمي والتقني
DIRECTION

+ 213 (0) 23 255 416 +213 (0) 23 255 410
05, Rue des trois Frères Aissou
Ben Aknoun, BP 143, 16030 - Alger - Algérie
www.cerist.dz

+213(0) 23 255 416 +213(0) 23 255 410
05 شارع الإخوة عيسو الثلاث ص.ب 143.
16030بن عكنون - الجزائر
سيريست.الجزائر

PRÉAMBULE

Le présent cahier des charges a pour objet la sélection, par le Centre de Recherche sur l'Information Scientifique et Technique, d'un prestataire **spécialisé dans l'infogérance en cybersécurité (audit, surveillance continue et intervention en cas d'incident de sécurité).**

Aussi bien la lettre de consultation que l'ensemble de la procédure de désignation du prestataire obéissent aux dispositions des textes légaux en vigueur notamment :

- Loi N°23-12 du 18 Moharram 1445 correspondant au 5 août 2023 fixant les règles générales relatives aux marchés publics,
- Décret présidentiel N°15-247 du 2 Dhou El Hidja 1436 correspondant au 16 septembre 2015 portant règlementation des marchés publics et des délégations de service public,

Les deux documents précités (la lettre de consultation et le cahier des charges) ont été diffusés sur le site web du Centre de Recherche sur l'Information Scientifique et Technique (CERIST).

I. Informations générales concernant l'établissement

1. Présentation de l'établissement

Crée en 1985 par décret N° 85-56 daté du 16 mars 1985, le Centre de Recherche sur l'Information Scientifique et Technique, communément appelé CERIST, est un organisme étatique à vocation intersectorielle. Sa principale mission est de mener des activités de recherche ayant pour objectif la mise en place et le développement d'un système national d'information scientifique et technique.

En 2003, le CERIST devient Etablissement Public à caractère Scientifique et Technologique (EPST) sous tutelle du Ministère de l'Enseignement Supérieur et de la Recherche Scientifique (MESRS).

Le CERIST est organisé en : quatre (4) unités de recherche, cinq (5) divisions de recherche, quatre (4) départements techniques, deux (2) services communs et trois (3) services administratifs, placés sous la direction d'un Directeur, appuyé par un Directeur Adjoint et d'un Secrétaire Général.

Ses missions ont été élargies notamment aux activités suivantes :

- Mener toute activité de recherche relative à la création, la mise en place et le développement du système national d'information scientifique et technique.
- Promouvoir la recherche dans les domaines des sciences et des technologies de l'information et de la communication et de participer à leur développement,
- Contribuer à la coordination et à la mise en œuvre des programmes nationaux d'information scientifique et technique dans un cadre concerté et en liaison avec les secteurs concernés,
- Contribuer à l'édification et à la promotion de la société de l'information par la mise en place et le développement de réseaux sectoriels d'information thématiques notamment le réseau académique et de recherche, et d'assurer la connexion avec les réseaux similaires à l'étranger ainsi que par le développement et la généralisation des techniques d'information et de communication dans les activités d'enseignement supérieur,
- Participer à la modernisation du système documentaire universitaire national par la mise en place notamment de bibliothèques virtuelles,
- Réunir les éléments nécessaires à la constitution de bases de données nationales dans les domaines des sciences et de la technologie et en assurer la diffusion,
- Promouvoir la recherche en matière de sécurité de l'information et des réseaux.

Le CERIST est doté de la personnalité morale et de l'autonomie financière, il est soumis depuis 2011 aux dispositions du décret exécutif n°11-396 du 28 Dhou El Hidja 1432 correspondant au 24 novembre 2011 fixant le statut-type de l'établissement public à caractère scientifique et technologique.

II. Caractéristiques techniques de la solution attendue

La prestation demandée est une prestation d'infogérance en cybersécurité (audit, surveillance continue et intervention en cas d'incident de sécurité) couvrant le périmètre d'un (01) projet OpenStack (équivalent d'un Virtual Private Cloud ou Virtual Private DataCenter) composé d'un ensemble de sept (07) machines virtuelles (instances) et protégées par un Firewall virtuel et d'un WAF virtuel en plus d'un Firewall physique.

La prestation demandée doit couvrir les services suivants :

a) **Configuration, optimisation et réglages fins du WAF virtuel (FortiWeb)**
b) **Audit sécuritaire des configurations et de l'architecture du périmètre**
c) **Surveillance Continue et Intervention en cas d'incidents de Sécurité selon les modalités suivantes**

- **Surveillance sécuritaire continue avec une couverture 24h/24, 7 jours/7 afin de détecter tout incident de sécurité.**
- **En cas d'incident de sécurité, prise en charge les incidents de sécurité détectés suivant les modalités de signalement et d'intervention ci-dessous :**

Fenêtre de signalement	**24x7**
Réponse initiale	**…. Minutes**
Intervention à distance	**…. Heures**
Intervention sur site	**…. Heures sur Alger**
Debriefing quotidien	**Jusqu'à la clôture de l'incident**
Rapport final	**Après la clôture de l'incident**

d) Configuration et mise à disposition d'un Dashboard (SIEM) adapté et personnalisé pour la surveillance continue des événements relatifs au périmètre défini dans le cadre de cette consultation

III. Conditions et critères de soumission

Le soumissionnaire doit avoir les compétences techniques requises pour mener à bien ce type de mission, à travers des certifications de ses intervenants dans les divers domaines objets de la présente consultation ainsi que les moyens techniques utilisés et mis à disposition.

Le soumissionnaire indiquera dans son offre le nombre d'intervenants affectés à la réponse d'incidents et leur organisation pour garantir l'exigence d'une couverture 24/7.

Il est exigé que les intervenants soit 100% de nationalité algérienne.

IV. Tableau d'évaluation

Item	Détails	Réponse
Configuration, optimisation et réglages fins du WAF virtuel (FortiWeb)		Oui/Non
Audit sécuritaire des configurations et de l'architecture du périmètre		Oui/Non
Surveillance Continue et Intervention en cas d'incidents de Sécurité		
Déploiement des sondes de surveillance et configuration de l'envoi des Logs et des événements		Oui / Non
Surveillance sécuritaire continue avec une couverture 24h/24, 7 jours/7 afin de détecter tout incident de sécurité.		Oui / Non
En cas d'incident de sécurité, prise en charge les incidents de sécurité détectés suivant les modalités de signalement et d'intervention ci-après	Incident Response	Oui/Non
	Fenêtre de signalement : 24x7	
	Réponse initiale	… minutes ou … heures
	Intervention à distance	… heures
	Intervention sur site	… heures
	Debriefing quotidien Jusqu'à la clôture de l'incident	Oui/Non
	Rapport final après la clôture de l'incident	Oui/Non
	Advanced Incident Response Si Oui : Indiquer le nombre total d'heures	Oui/Non

Caractéristiques du SIEM	Hébergé au niveau national	Préciser l'emplacement de l'hébergement
	Durée de rétention des logs et des événements	Nombre de jours
	Prevention anti-Malware, Ransomware	Oui/Non
	Rule-based Detection and/or AI-based Detection	Oui/Non
	Mise à disposition d'un Dashboard dédié et personnalisé au périmètre sécurisé	Oui/Non et caractéristiques
Capacités humaines		
Nombre, qualifications et nationalité des intervenants et leurs organisation dans le cadre de la prestation demandée	Fournir les CVs des intervenants et leurs certifications	
Certifications en « Incident Response »	Indiquer le nombre de certifications (avec justificatifs)	
Certifications en Offensive Security Certified Professional (OSCP)	Indiquer le nombre de certifications (avec justificatifs)	
Certifications en Offensive Security Web Expert (OSWE)	Indiquer le nombre de certifications (avec justificatifs)	
Certifications en Offensive Security Experienced Penetration Tester (OSEP)	Indiquer le nombre de certifications (avec justificatifs)	
Certifications en Certified Red Team Expert (CRTP)	Indiquer le nombre de certifications (avec justificatifs)	
Autres certifications équivalentes	Indiquer le titre, le nombre et présenter les justifications	
Références (attestations de bonne exécution)		
Attestations de bonne exécution en matière de réponse aux incidents		
Attestations de bonne exécution en matière d'Audit de sécurité		

V Respect des échéances

Le soumissionnaire s'engage à suivre le plan de travail soumis au CERIST en veillant au respect des délais pour lesquels il s'est engagé.

VI Prix et conditions de paiement

VI .1 Prix

Les prix sont fermes et non révisables durant toute la durée du contrat.

VII Modalités de paiement

Le règlement des dus s'effectue sur présentation de factures et après constat du service fait.

VIII Date et heure limites de remise de l'offre

Le dernier délai de dépôt des offres est fixé pour la journée du 30/10/2024 **à 12h00** de ce fait les fournisseurs disposent de **10 jour pour préparer leurs offres.**