CATALOGUE DE SERVICES ET SOLUTIONS

pour un accompagnement global en cybersécurité des institutions publiques de la province de Luxembourg via la centrale d'achat IDELUX Projets publics

IDELUX PROJETS PUBLICS

easi network srl

RHEA GROUP

Table des Matières

IDELUX
PROJETS PUBLICS

À l'heure où les administrations, organismes et collectivités sont invités à penser tout-numérique et à mettre en place de nouveaux canaux de communication avec les usagers, la forte croissance et la complexification des menaces cyber, en perpétuelle mutation, font peser de nouveaux risques sur les services publics (villes, communes, hôpitaux, collectivités).

L'accord-cadre IDELUX Projets publics, portant sur l'accompagnement global en cybersécurité des institutions publiques de la province de Luxembourg, s'inscrit dans la volonté de proposer aux pouvoirs publics des services et solutions pour anticiper et réduire les risques de cyber attaques.

Ce catalogue de services et solutions est mis à la disposition des institutions publiques opérant sur le territoire de la province de Luxembourg. Il liste les services et solutions dont elles peuvent bénéficier, dans le cadre de l'accord-cadre IDELUX Projets publics, les démarches à suivre pour en bénéficier, les partenaires recommandés par les opérateurs pour le déploiement des solutions, ainsi que les points de contact au sein des opérateurs principaux.

Ces services et solutions sont fournis par l'opérateur principal, l'association momentanée formée par RHEA S.A. et EASI Network S.A.RL.

SERVICES DE CYBERSÉCURITÉ

Audit de sécurité (Gouvernance, risque et conformité)

L'audit de sécurité a pour but de vérifier la gestion des risques en matière de sécurité informatique au sein des institutions publiques, notamment en vérifiant la politique de sécurité, les plans de continuité d'activité, etc. Cela permet de réduire les risques de cyberattaques.

RHEA Group vous accompagne dans la réalisation de l'audit qui conduira à un rapport détaillé précisant les améliorations à apporter. Les audits de sécurité sont réalisés selon les référentiels de la norme ISO 27001 et assurent à votre organisation publique la mise en place d'une gouvernance répondant à des exigences légales et réglementaires.

Audit de l'infrastructure IT

L'audit technique de l'infrastructure permet, en partant de zéro, d'avoir une connaissance précise de l'ensemble des équipements connectés au réseau de l'entreprise. Un audit de l'infrastructure IT permet d'identifier ses fragilités, qu'elles soient structurelles (manque de redondances, de sauvegardes) ou élémentaires (obsolescence matérielle ou logicielle). A l'issue de cet audit, un rapport précis et détaillé est remis sur la situation existante et les recommandations d'améliorations pour remédier à des manquements ou carences identifiés pour la sécurité de vos actifs.

Pen Test

Les Pen Tests (tests d'intrusion) permettent, par des simulations d'attaque informatique en conditions réelles, de rechercher les vulnérabilités présentes sur le réseau, l'infrastructure et les applications. Les différents Pen Tests qui sont proposés permettrons de mettre en avant l'exposition de votre organisation aux différents risques cyber existants. Ils pourront être de type

boite noire, boite blanche ou boite grise.

Après la réalisation du test, un rapport est rédigé et présenté au bénéficiaire. Ce rapport final décrit les vulnérabilités identifiées et classées par ordre de priorité “critiques”, “élevées”, “moyennes” ou “faibles”, ainsi que les recommandations pour y remédier. Ces niveaux de criticité sont établis selon le système actuel de notation des vulnérabilités communes (CVSS)

Scan de Vulnérabilité ‘as a service’

Dans le cadre des services gérés d’analyse des vulnérabilités, RHEA se charge du déploiement, de la mise en œuvre, et de la gestion de la solution d’analyse des vulnérabilités. Cela comprend des tâches telles que la configuration du système, le déploiement d’agents et la mise à jour de la solution au fur et à mesure que de nouvelles menaces et vulnérabilités sont découvertes.

Les services gérés de RHEA pour les analyses de vulnérabilité s’adressent aux organisations publiques de toutes tailles. Ils permettent d’identifier et de remédier aux vulnérabilités des infrastructures informatiques des organisations avant qu’elles ne puissent être exploitées par des cybercriminels.

Le Scan de Vulnérabilité est un service 24/7 géré par les équipes du SOC (Security Operation Center) de RHEA qui assure les services de déploiement de la solution, de la mise en place de la politique de patching et de la présentation d’un rapport détaillé mensuel.

EDR ‘as a service’

L’Endpoint Detection Response (EDR) est un ensemble d’outils de cybersécurité conçus pour détecter et supprimer tous les malwares, ou tout autre activité malveillante, dirigés contre les terminaux connectés à votre réseau d’entreprise.

Avec les services EDR gérés, RHEA se charge du déploiement, de la mise en œuvre, de la surveillance et de la gestion de la solution EDR. Cela inclut des tâches telles que la configuration du système, le déploiement d’agents et la mise à jour de la solution au fur et à mesure que de nouvelles menaces et vulnérabilités sont découvertes.

Ce service est assuré en 24/7 par les équipes de RHEA.

XDR ‘as a service’

XDR ‘as a service’ permet aux clients d’exploiter les capacités avancées de la plateforme XDR (Extended Detection and Response) pour détecter et répondre aux cybermenaces sur l’ensemble de leur surface d’attaque, y compris les terminaux, les réseaux, le cloud et les applications SaaS.

Avec les services XDR gérés, RHEA s’occupe du déploiement, de la mise en œuvre, de la surveillance et de la gestion de la solution XDR. Cela inclut des tâches telles que la configuration du système, le déploiement d’agents et la mise à jour de la solution au fur et à mesure de la découverte de nouvelles menaces et vulnérabilités.

Ce service est assuré en 24/7 par les équipes de RHEA.

Service de réponse aux incidents

Pour endiguer une attaque et limiter son pouvoir de nuisance, il faut y répondre rapidement et l'analyser sous toutes ses coutures. La réponse aux incidents doit pouvoir être mis en place quel que soit la taille de l'organisation publique.

Le service de réponse aux incidents de RHEA fournit aux clients une solution complète de réponse aux incidents (cyberattaques) couvrant tous les aspects de la gestion des incidents, de la détection et de l'analyse au confinement, à l'éradication et à la récupération. En outre, il fournit une politique de gestion de crise complète qui comprend des processus et des détails opérationnels pour gérer l'incident du début à la fin.
Ce service de réponse aux incidents s'inscrit dans le cadre de la mise en place et du test d'un plan complet de réponse aux incidents.

Mise en place et test d'un plan de réponse aux incidents

L'objectif d'une gestion des incidents est d'être préparé en cas d'interruption imprévue. Savoir qui fait quoi, qui avertit qui, par quels moyens, et quand, vous permet de gagner un temps précieux.

La politique de gestion de crise comprend des procédures de :
• réponse à l'incident,
• escalade de l'incident,
• communication et notification de l'incident,
• rétablissement après l'incident.

La politique de gestion de crise précise également la façon dont l'incident sera traité, les responsabilités de chacun et les mesures à prendre pour minimiser l'impact de l'incident sur l'organisation.


MAX

SOLUTIONS DE PRÉVENTION, DE DÉTECTION ET DE PROTECTION DES RISQUES CYBER

Protection du réseau avec la suite d'outils de sécurité AXS Guard

AXS Guard est une plateforme de cybersécurité complète et évolutive qui convient à toute entreprise ou organisation, grande ou petite.

Les solutions proposées comprennent les Firewall, le VPN, le Secure DNS et les Web Appliance Firewall.

Protection des boites mails avec la solution Vade

Des solutions de sécurité des emails pour toutes les entreprises. Vade protège vos collaborateurs, vos activités et vos clients contre les menaces de cybersécurité avancées, notamment le phishing, le spear phishing et les malwares. La solution Vade est disponible pour votre environnement Microsoft 365 et dans le cloud.

Protection des accès et authentification forte

La plupart des cyberattaques ont pour origine le vol et l'utilisation frauduleuse de données d'identification. L'authentification multifactorielle (MFA) est une contre-mesure efficace tant que le niveau de sécurité offert par la solution n'est pas compromis. Les solutions AFRILAS et TRUSTBUILDER vous assurent une sécurité des accès par le déploiement d'une solution 2FA (2 facteurs d'authentification) simple à déployer et facile d'utilisation pour les utilisateurs.

Protection des terminaux mobiles

Une flotte mobile, qu'elle soit composée de terminaux professionnels ou personnels, est une porte d'entrée vers le système d'information des entreprises. La solution Pradeo protège les terminaux mobiles (smartphones, tablettes…), les applications et les données. La technologie "Mobile Threat Defense" est dédiée à la protection des terminaux mobiles des membres d'une organisation publique, afin qu'ils ne deviennent pas la source d'une faille de sécurité.

Solution Antimalware

L'antimalware de ESET est conçu pour empêcher, détecter et éradiquer les programmes malveillants, aussi bien sur les ordinateurs individuels que dans les systèmes informatiques. ESET Protect Advanced offre plusieurs couches de protection et peut détecter les logiciels malveillants avant, pendant et après leur exécution ainsi qu'un système d'analyse proactif pour les fichiers inconnus et les nouvelles menaces.

Solution EDR

La solution EDR Inspect est un complément de la solution antimalware. Elle offre une couche de sécurité supplémentaire des terminaux (PC et serveurs) avec des fonctionnalités de détection et de remédiation des malwares. ESET Inspect remonte l'ensemble des informations relatives à l'activité des machines et les mets en corrélation avec des règles de détection qui se basent sur l'expertise de l'éditeur et sur le framework MITRE ATT&CK.

Solution de partage de fichiers

La solution Oodrive work permet de sécuriser les échanges de fichiers sensibles en interne entre collaborateurs mais aussi vers des partenaires externes. Vous assurez ainsi une traçabilité et un niveau de sécurité élevé pour tous vos échanges de fichiers.

Solution de signature électronique

La signature électronique est un processus numérique permettant de signer en ligne tous types de documents en leur accordant une valeur probante et un archivage sécurisé. En optant pour ce processus dématérialisé de création de signature électronique en ligne, les étapes de signature se simplifient, se réduisent et sécurisent davantage vos consentements.

Solution de gestion de réunions stratégiques

Avec Oodrive, organisez des réunions efficaces grâce à des outils de planification et de visioconférence qui ouvrent les discussions dans un environnement totalement sécurisé. Oodrive Meet facilite l'organisation d'une réunion à distance, depuis la recherche de l'horaire qui convient à tous les participants, à la compilation des documents en vue de leur supervision, jusqu'à la communication des comptes-rendus. Le tout dans un environnement sécurisé.

Scan de vulnérabilités

En 2022, plus de 65 000 vulnérabilités ont été détectées au niveau mondial.Cyberwatch Vulnerability Manager permet d'identifier les éléments présents dans les systèmes d'information grâce à un moteur de découverte d'actifs. Cyberwatch cartographie la liste complète et contextualise les vulnérabilités présentes dans de votre parc informatique.

Campagne de sensibilisation

La maturité des employés aux risques d'attaques cyber est très disparate suivant les tailles des organisations, le profil et la formation des employés. La formation et la sensibilisation des collaborateurs aux risques cyber est donc un enjeu important.

La solution informatique "Avant de cliquer" offre une solution de sensibilisation complète sous forme d'une plateforme web intégrant :

- Du e-learning avec un grand nombre de modules de cours sur la cyber sécurité et le RGPD
- Une solution de phishing automatisée
- Un bouton "Alert Phishing" offrant la possibilité de remonter des alertes vers l'équipe informatique

COMMENT BÉNÉFICIER DE CES SERVICES ET SOLUTIONS ?

Toute institution publique opérant sur le territoire de la province de Luxembourg (communes, CPAS, intercommunales, Province, zones de police, zone de secours...) peut bénéficier des services et solutions prévus dans l'accord-cadre IDELUX Projets publics.

La durée du marché s'étale jusqu'au 24 mai 2027 ou 2.000.000 EUR de commandes.

Si vous avez déjà adhéré à la centrale d'achat IDELUX Projets publics

Si les pouvoirs publics ont déjà adhéré à la centrale d'achat IDELUX Projets publics pour des machés-cadres conclus antérieurement, les bénéficiaires sont invités à suivre les étapes suivantes pour passer la commande :

- Décision de l'organe décisionnel compétent de passer commande (suivant le montant estimé du marché)
- Rédaction du formulaire de demande d'offre avec IDELUX Projets publics et envoi par mail à l'opérateur principal du marché
- Remise d'offre par l'opérateur principal dans les 15 jours de calendrier par mail
- Analyse et proposition d'attribution de l'offre par IDELUX Projets publics
- Notification du marché par courrier et par email

Au vu de la spécificité des services et solutions, les bénéficiaires doivent recourir à l'assistance obligatoire d'IDELUX Projets publics à chaque étape.

Si vous n'avez pas adhéré à la centrale d'achat IDELUX Projets publics

Si les pouvoirs publics n'ont pas déjà adhéré à la centrale d'achat IDELUX, les bénéficiaires sont invités à suivre préalablement les étapes suivantes :

- Obtenir la convention d'adhésion à la centrale d'achat auprès d'IDELUX Projets publics.
- Valider la convention d'adhésion par l'organe décisionnel compétent (Conseil communal, Conseil d'Administration,)

L'adhésion à la centrale d'achat est libre et non exclusive.

Votre personne de contact chez IDELUX Projets publics

Benoît Muller
benoit.muller@idelux.be
+32 63 231 889

POUR VOUS ACCOMPAGNER DANS SES SERVICES

Nous avons sélectionné les partenaires suivants :

RHEA Group :
Audit de sécurité, Pen test, services managés et réponse à l'incident

EASI Network :
Audit d'infrastructure, déploiement et intégration des solutions proposées

AXSGUARD :
Protection du réseau

VADE :
Protection des boites mails solutions anti phishing, ransomware, spear phishing

PRADEO :
Protection des terminaux mobile et des applications mobiles

OODRIVE :
Solution de partage de fichiers, de signature électronique et de gestion des réunions

AVANT DE CLIQUER :
Solution de sensibilisation des collaborateurs et de campagnes de phishing automatisées

CYBERWATCH :
Scan de vulnérabilités

ESET :
Antimalware et EDR pour la sécurisation des terminaux (pc)et serveurs

AFRILAS :
Solution d'authentification forte

TRUST BUILDER :
Solution d'authentification forte

Tous les partenaires, éditeurs sont européens et vous assurent des solutions souveraines.

DEMANDE D'INFORMATION

Vos personnes de contacts au sein des opérateurs principaux pour toute demande d'informations :

RHEA Group
Fabrice Hecquet
f.hecquet@rheagroup.com
Tel : +32 478 820 303

Easi Network
Eric Ansenne
eric.ansenne@easinetwork.be
Tel : +32 495 569 045