maguen

CYBER

MAKING YOUR BUSINESS SECURE !

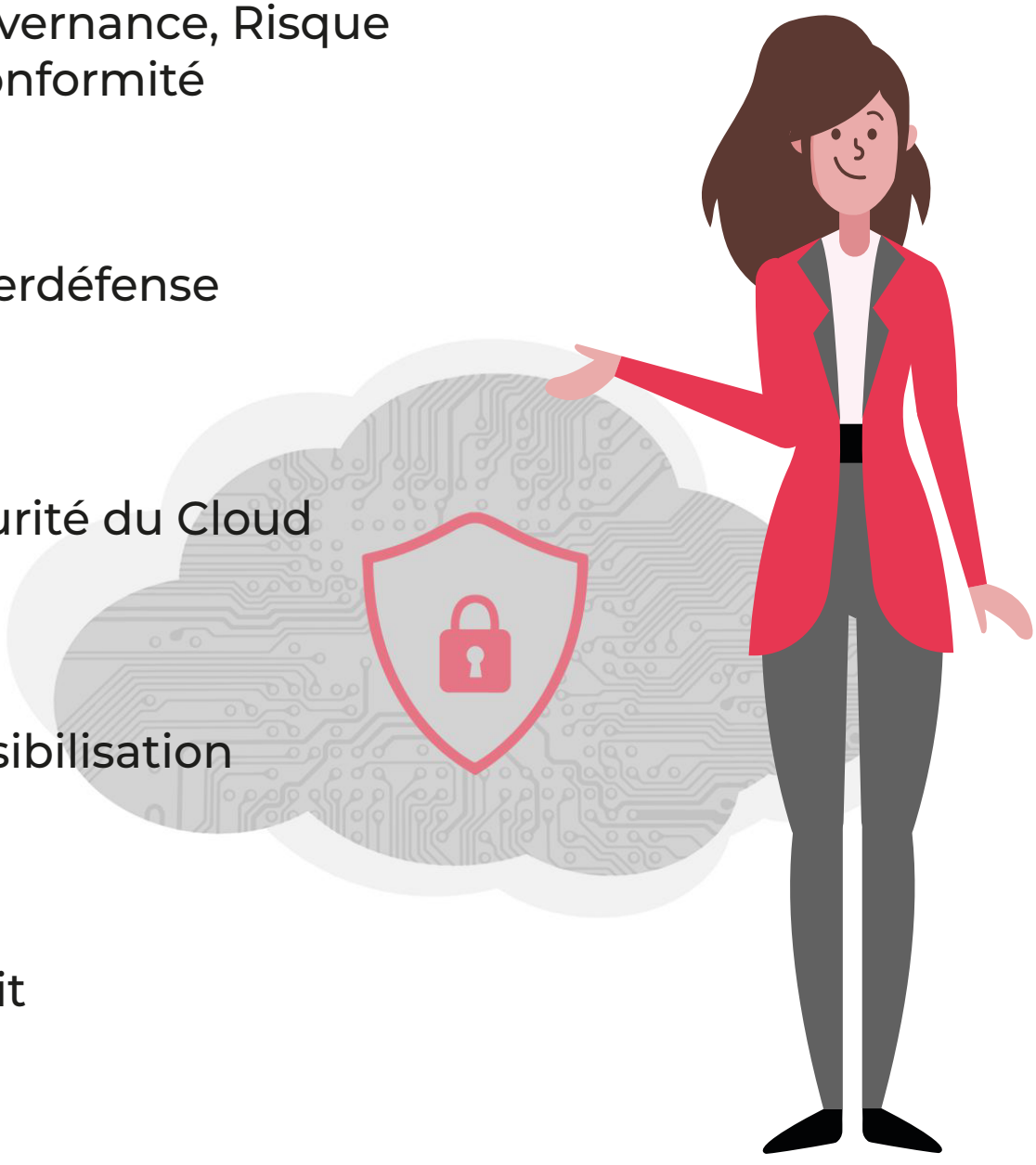
Gouvernance, Risque & Conformité

Cyberdéfense

Sécurité du Cloud

Sensibilisation

Audit



Notre philosophie, nos valeurs et notre expertise dans le domaine de la cybersécurité vous apportent notre compréhension et notre capacité à imaginer les meilleurs moyens d'augmenter votre sécurité sur les données appartenant à votre entreprise. Chez Maguen Cyber, notre plus value est la mise en place d'un accompagnement après l'installation d'une solution adaptée et personalisée à votre structure.

Intégration de la sécurité dans le projet (ISP)

Conduit des programmes ou des projets et délivre des solutions de sécurité
Supervise le respect du calendrier et du budget
Gère les risques programme ou projet
Communique et reporte sur l'avancement, les livrables et les risques
Rédaction de PSSI / Procédures / Intégration / Suivi d'indicateurs

Assistance et Accompagnement au RSSI

Structuration d'un programme et d'une Roadmap sécurité
Renfort des fonctions SSI
Amélioration et déploiement des dispositifs de contrôle
Intégration des périmètres Cloud et Agile
Transformation de la filière pour créer de la valeur au bénéfice de nos clients

Conformité

Gap Analysis : analyse d'écarts entre l'existant et la cible sécuritaire
Définition d'un plan d'action avec l'inventaire et cartographie des chantiers prioritaires
Construction d'une gouvernance adaptée au contexte du client et rédaction de la documentation nécessaire à l'organisation pour la mise en oeuvre de la réglementation
Mise en place des axes d'améliorations préconisés dans le rapport d'audit à travers du conseil ou de l'intégration de solutions
Conseil et expertise auprès des métiers pour les aider à intégrer les recommandations dans leurs Roadmap SSI

Gestion des risques opérationnels

Élaboration et mise en place d'une gouvernance de la sécurité et du risque opérationnel pour la maîtrise des risques
Cartographie et identification des risques à travers différentes approches
Évaluation des risques selon différents critères (gravité, détection/gestion, occurrence,...)
Élaboration du plan de traitement des risques
Surveillance des risques avec la mise en place d'un dispositif de suivi et de contrôle du profil de risque de l'entreprise
Élaboration d'un outillage d'analyse et de traitement des risques dynamique, prenant en compte les changements du SI dans le temps

Réponse à incident et Forensic

Forensics et Investigation sur les traces d'activité (applications, ordinateurs et réseaux)

Centre de sécurité opérationnel (SoC)

L'étude de la mise en place d'une organisation d'un SoC et d'outils SIEM
(Architecture / Gouvernance / Exploitation)
La mise en place d'une stratégie de surveillance sur les différentes couches de votre système d'information de poste de travail au Cloud

Renseignement menace Externe (Threat Intelligence)

Hunting et recherche des signaux faibles et des marqueurs de compromissions (IOC)
Analyse contextuelle et stratégique contenant une description des secteurs industriels et géographiques touchés

Automatisation et outillage (DevSecOps)

L'approche DevSecOps, permet d'assurer les hauts standards de qualité même pour les méthodes de développement agiles et rapides de livraison continue et d'intégration continue. Dans ces cas, les exigences de sécurité, souvent très élevées, doivent être prises en compte lors de la programmation de l'exploitation courante.

Maguen Cyber offre une solution avec son partenaire **Rezilion** « plateforme DevSecOps qui élimine le travail manuel nécessaire pour protéger les applications contre les vulnérabilités et les menaces.

- Réduction des efforts de correction des vulnérabilités jusqu'à 70 %.

- Fournir aux RSSI la surface d'attaque réelle par rapport à une surface d'attaque perçue, leur permettant de mieux allouer les ressources.

- Trouvez plus de temps pour corriger sans ralentir les opérations commerciales en fournissant des contrôles compensatoires pour les vulnérabilités de production grâce à une atténuation autonome.

Azure Sentinel · ATT&CK · OPENCTI · rezilion · splunk> · ArcSight · TheHive · Cortex · elastic · Cyberint · IBM QRadar

Infrastructure sécurisée - Cloud

Sécurité Périmétrique

- Gestion de projet technique et fonctionnel
- Architecture, intégration et optimisation d'infrastructure système, réseaux et sécurité
- Réalisation de la production et de l'exploitation des outils de sécurité périmétrique

Sécurité du Cloud

- Accompagnement pour la conception d'architecture Cloud sécurisée
- Mise en place d'outillage de sécurité des accès à vos infrastructures Cloud (CASB, SWG,...)
- Mise en place d'outils de protection des données dans le Cloud (DLP, chiffrement, -transfert sécurisé,...)

Protection des terminaux (EndPoint)

- Accompagnement dans la définition de la politique de sécurisation de vos EndPoints.
- Implémentation de solutions spécifiques (antivirus, chiffrement de disque, DLP, EDR)

Protection des Accès (IAM)

- Définition des politiques de gestion des accès
- Gouvernance et administration des identités (IGA)
- Accompagnement pour la conception et l'intégration de solution de gestion des identités -et des accès IAM

bitglass, netskope, proofpoint, FORTINET, paloalto NETWORKS, Forcepoint, RAPID7, CISCO, Azure Active Directory, vmware Carbon Black., CROWDSTRIKE, okta, SentinelOne, Nucleon Protect data that matters

Formation d'initiation à la sécurité

- Cadrage de la formation au travers d'ateliers afin de réaliser un état des lieux de l'existant
- Identifier les profils à former
- Valider le planning de formation
- Quizz de fin de sensibilisation
- synthèse des résultats du quizz

Campagne de hammeçonnage

- Campagne d'envoi d'emails avec un lien, (faire un site externe imitant les applications de l'entreprise demandant de saisir les identifiants)
- Campagne d'envoi d'emails demandant à installer un nouveau logiciel
- Envoi d'accessoires piégés au poste de travail
- Appel des personnes afin d'effectuer des manipulations sur leur postes de travail
- Action sur site focalisée sur une équipe précise par la persuasion orale : personnel d'accueil, veilleur de nuit, administrateur système

Campagne de sensibilisation ludique

- Définition et mise en place d'une stratégie de sensibilisation adaptée
- Création de programme de sensibilisation
- Exercices ludiques avec mises en situation réelle en adaptant les messages au contexte des équipes
- Mise à disposition de contenue de sensibilisation (fiche réflexe, infographie, jeux vidéo, ...)

audit de Social Engineering

Les consultants audit de Maguen Cyber peuvent adopter une approche offensive et de sensibilisation en contextualisant leurs attaques (USB dropper, phoning, etc.).

Scan de vulnérabilité

- De détecter les risques et vulnérabilités grâce à des outils de scan de vulnérabilités (Nessus Tenable, Qualys, ...)
- De prioriser les vulnérabilités et d'analyser l'impact sur les opérations sur la base de différentes sources externes

Test d'intruision (PenTest)

- Evaluation de la sécurité du périmètre défini suivant une méthodologie spécifique aux périmètres testés, qui s'appuie notamment sur le PTES (Penetration Testing Execution Standard), ainsi que sur des ressources fondamentales telles que l'OWASP.
- Un rapport d'audit clair et détaillé est rédigé à la suite de la prestation, mentionnant les points positifs et les préconisations nécessaires pour pallier les éventuelles vulnérabilités. La restitution de ce rapport pentest correspond à une présentation téléphonique ou dans vos locaux et se décompose ainsi :
    - Restitution managériale
    - Restitution technique
    - De réaliser des actions correctives sur les infrastructures réseau, Web, Cloud, en fournissant une analyse des risques contextuelles et des rapports en phase avec les obligations réglementaires et industrielles

Audit de code

On peut découper l'audit de code en quatre étapes.

1. Préparation : Définir les objectifs pour mieux cibler l'audit : vulnérabilités, maintenabilité, performance et/ou conformité...
2. Revue Automatique : une analyse automatisée du code est effectuée.
3. Revue Manuelle : les modules de l'application les plus sensibles sont revus manuellement.
4. Restitution : c'est une étape essentielle ! Un audit est inutile s'il n'est pas suivi de corrections.

Le livrable contient aussi des remarques et conseils afin d'améliorer les documents techniques. Il peut aussi servir de base pour de futurs audits.

Test d'intruision avancé RedTeam

L'audit RedTeam reprend toutes les possibilités offertes lors des audits d'infrastructure et d'application web ou mobile et en plus les actions et conditions suivantes :

- Sur un large périmètre.
- Durée du test étendue sur plusieurs semaines.
- Peut inclure des intrusions physiques et du social engineering.
- Peut inclure du reverse de binaires trouvés.
- Peut inclure l'installation d'outils de pénétration sur plusieurs semaines.
- Peut inclure des attaques sur des équipements de sécurité.
- Peut inclure l'utilisation d'identifiants privilégiés obtenus durant les tests.

Nos Talents

Notre philosophie de Ressources Humaines est orientée vers un suivi personnalisé et une garantie de disponibilité pour nos collaborateurs.
Maguen Cyber développe, ainsi un modèle d'employeur humain et ambitieux qui fédère ses équipes autour de valeurs fortes :

- La culture de l'excellence
- L'engagement
- Le mérite

Nos talents, des ingénieurs spécialisés dont le potentiel est optimisé par une gestion des carrières de l'entreprise. Cette politique nous permet de favoriser l'évolution horizontale ou verticale de nos collaborateurs, mais aussi de proposer à nos clients un regard toujours plus expert sur leurs activités

Notre engagement RSE

Nous avons à cœur de développer une politique de Responsabilité sociale et environnementale raisonnée dans un contexte d'évolution technologique en perpétuel mouvement. En tant qu'acteur majeur de l'informatique, nous entamons une démarche qui vise à réduire considérablement l'empreindre écologique, économique et sociale de nos réseaux dans les SI de nos clients.

Charte diversité

Inscrite dans la politique globale de Maguen Cyber, la Charte de la diversité a pour objet de favoriser l'égalité des chances et la diversité dans toutes ses composantes. La charte de la diversité contribue à développer un management respectueux des différences et fondé sur la confiance.
Elle améliore la cohésion des équipes, sources d'un meilleur vivre ensemble et donc de performance.

Charte fournisseurs

Maguen Cyber est engagé dans une démarche de responsabilité sociétale comme définit dans le Pacte Mondial des Nations Unies et souhaite que ses collaborateurs, fournisseurs, prestataires et partenaires soient partie prenante de cette démarche en signant cette charte.

maguen

CYBER

9/11 Avenue Saint-Mandé
Paris, 75012

www.maguen-cyber.fr
contact@maguen-cyber.fr
01 53 43 89 34