RSECURE

Méthodologie H.O.P.

Adoptez une méthodologie simple et efficace pour rester à l'abri des risques cyber !

MADE IN LUXEMBOURG

Avec la croissance constante de la digitalisation des entreprises, la protection des données sensibles et des réseaux informatiques contre les intrusions est devenue une priorité pour éviter tous types de cyberattaques.

L'objectif de l'approche H.O.P. est de soutenir les entreprises dans l'amélioration continue de leur maturité cybernétique, tout en tenant compte de sa taille et de son secteur d'activité, sur la base des 3 points suivants : les **Humains**, les **Outils**, et les **Processus**.

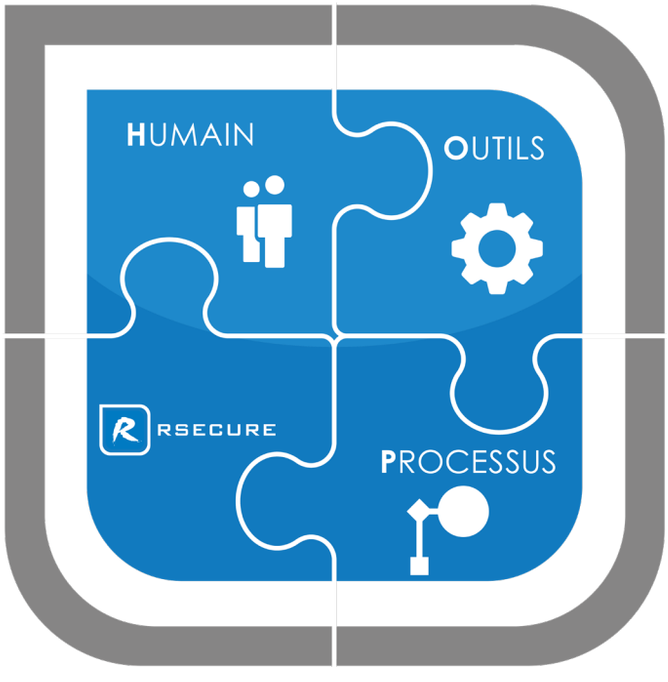
HUMAIN

Conscientiser l'humain :

Sur le plan humain, vos collaborateurs doivent être sensibilisés aux risques liés à votre environnement informatique. Notre équipe d'experts réalise des formations en présentiel ou en ligne pour vous permettre de détecter les menaces et d'y répondre !

Notre approche :

- Former les équipes à détecter les menaces existantes et à y répondre le plus efficacement possible,
- Sensibiliser en continue les collaborateurs,
- Tester les employés après la formation.



Rsecure SARL / www.rsecure.lu
38-40, Parc d'Activités L-8308 Capellen

OUTILS

Se doter des meilleurs outils du marché :

En plus des formations de vos utilisateurs, nous aidons les entreprises à investir dans les outils de sécurité appropriés. Nous pouvons recommander des solutions de pare-feu, des logiciels antivirus, des outils de détection d'intrusion, des solutions de chiffrement et d'autres technologies pour protéger vos systèmes informatiques contre les menaces potentielles.

Aussi, nous travaillons avec vous pour comprendre les vulnérabilités de votre infrastructure informatique et les menaces auxquelles votre entreprise est exposée. Cette évaluation permet d'identifier les mesures de sécurité nécessaires pour protéger votre entreprise contre les attaques potentielles.

Quelques exemples d'outils (liste non exhaustive) :

- Gestion des accès à privilèges
- Signature électronique
- Identification et blocage des tentatives d'attaques basés sur les technologies d'intelligence artificielle auto-apprenante
- Cybermonitoring de votre infrastructure IT
- Tests de pénétration
- Les indispensables, tels que antivirus, antispams, encryption des données et tant d'autres !

PROCESSUS

Définir des processus pour optimiser la sécurité :

Notre équipe professionnelle en cybersécurité rédige et met à votre disposition les processus dont vous avez besoin pour une sécurité optimale.

- Politiques : nos experts vous accompagnent dans la rédaction et la mise en place des procédures et politiques d'entreprise afin de garantir une exécution des tâches en toute sécurité (exemple : DRP).
- Analyse de maturité : nous analysons votre maturité cyber à différents standards. Sur base de l'auto-évaluation, nous élaborons un plan d'action personnalisé pour vous aider à pallier les lacunes identifiées.
- CISO as a Service : externalisez le pilotage de la sécurité de votre environnement informatique avec nos services de CISO à la demande! Notre CISO se chargera de l'analyse des risques, de la maintenance des registres, et vous conseillera sur tous les aspects liés à la cybersécurité. Il vous accompagne mensuellement et met en place la méthodologie H.O.P au sein de votre entreprise !
- Gestion et analyse de risques

Afin de vous aider dans ce monde de régulations et certifications, nos experts certifiés proposent des services de mise en conformité aux différents standards européens et internationaux, tels que : NIS2, ISO27001, ISO27005, DORA, CSSF, ...

Nos professionnels travaillent avec vous pour définir des politiques claires et précises pour la gestion des mots de passe, l'accès aux informations personnelles, la gestion des appareils mobiles, la politique de sauvegarde des données et la sécurité des applications.