



La preuve par l'exemple !

- Un organisme public pour lequel l'**audit du firewall** a permis de mettre en évidence une faille majeure au niveau des règles de sécurité.
- Un fabricant d'accessoires de cuisine pour lequel un **audit de vulnérabilité interne** a permis de détecter une mauvaise configuration de l'un des serveurs qui occasionnait une surconsommation de 150% sur l'un des liens WAN.
- Un ASP, à la demande d'une grande compagnie financière, l'**évaluation de la politique de sécurité** a permis de découvrir une absence de procédures autour de l'administration des systèmes d'informations.
- Un fabricant de pièces automobiles. Un **audit de vulnérabilité interne** a permis de mettre en avant la non conformité des versions de patches de tous les serveurs (ceci occasionnait des "dysfonctionnements" aléatoires).
- Un fabricant de produits capillaires, l'**audit de vulnérabilité externe** a mis en évidence une grave défaillance de la plateforme antivirale.
- Un éditeur de logiciels pour lequel l'**audit du firewall** a permis d'éviter l'obtention d'informations depuis l'extérieur, l'**audit de vulnérabilité externe** a mis en évidence l'utilisation d'une version obsolète du relais de messagerie (risque de prise de contrôle depuis l'extérieur).
- Un laboratoire pharmaceutique pour lequel l'**évaluation de la politique de sécurité** a permis de mettre en évidence le non respect de la politique de sécurité pourtant existante.
- Une société de services dans le domaine de la "vente en ligne", l'**audit de la plate-forme d'accès internet** a mis en évidence la possibilité de prendre la main depuis un navigateur sur les consoles d'administration des machines publiques.

