



OCELOT

INVENTAIRE RÉSEAU ET ÉVALUATION DES
VULNÉRABILITÉS

**DANS CHAQUE RÉSEAU, IL Y A DES APPAREILS QUE
TOUT LE MONDE A OUBLIÉS.**

Un vieux NAS dans une armoire, une imprimante restée sur son firmware d'usine, un serveur de test que personne n'a jamais éteint. Tous font tourner des logiciels aux failles publiquement connues, et quiconque scanne le réseau peut les repérer.

L'inventaire tenu dans un fichier Excel ne correspond plus au réseau depuis longtemps, et personne n'a une semaine à consacrer à sa mise à jour manuelle.

Ocelot est un boîtier que vous branchez sur un port de switch. Il détecte tous les appareils actifs qu'il peut atteindre, recense les services que chacun expose et les compare à la base publique des CVE. Un agent sur les postes de travail y ajoute les logiciels installés.

Ocelot rédige ensuite le rapport : ce qui se trouve sur le réseau, ce qui ne va pas, la gravité de chaque constat et ce qu'il faut faire. Le branchement ne modifie en rien le réseau.

**QUELQU'UN SCANNERA VOTRE RÉSEAU.
FAITES-LE AVANT LUI.**

Un scan n'est qu'un instantané. Ocelot reste branché et lance des scans planifiés : un nouvel appareil ou une nouvelle vulnérabilité apparaît dans le prochain rapport, et non lors du prochain audit.

Chaque appareil reçoit un score de risque, ce qui permet d'appliquer d'abord les correctifs les plus urgents. L'historique fournit exactement ce que demande un auditeur ou un contrôle de protection des données : quand chaque problème a été détecté, et quand il a été résolu.



CE QUI EST INCLUS :

INVENTAIRE

Chaque appareil actif qu'Ocelot peut atteindre, avec son adresse, son fabricant (MAC), son nom d'hôte, son système d'exploitation et ses ports ouverts. Les appareils non documentés et les mauvaises configurations ressortent dès le premier scan.

LOGICIELS INSTALLÉS

Un agent sur chaque poste signale les applications installées et leurs versions : un navigateur ou un lecteur PDF obsolète figure ainsi dans le même rapport qu'un serveur non corrigé.

VULNÉRABILITÉS

Chaque service est comparé aux données CVE et reçoit un niveau de gravité. Les appareils sensibles peuvent être exclus du scan, afin de ne perturber aucun système critique. Pour la correction, les analystes d'EXYS peuvent passer en revue les résultats avec votre équipe.

PLANIFICATION ET RAPPORTS

Plusieurs scans récurrents, programmés en dehors des heures de bureau. Ocelot affiche une synthèse dès la fin d'un scan, puis envoie le rapport complet par e-mail : résumé pour la direction, tableaux d'inventaire, constats avec niveau de risque, détails techniques et recommandations.

CONTACTEZ-NOUS

ADRESSE

EXYS SA
Strada Regina 16
CH-6934 Bioggio
Tessin, Suisse

CONTACT

Tél. +41 (0)91 220 52 00

www.exys.swiss
office@exys.swiss

EXYS SA est certifiée ISO/IEC 27001



EXYS
WHERE PASSION
MEETS TECHNOLOGY
EXYS7600 - OCELOT