CF-Sentinel

FONCTIONNALITÉS CLÉS

- Découverte automatique de votre surface d'exposition à internet
- Détection des règles de pare-feu mal configurées
- Détection des services exposés à internet et des CVE impactant vos systèmes
- Détection de l'utilisation de mots de passe par défaut ou faibles
- Détection des fuites d'information

BÉNÉFICES CLÉS

- Pas d'installation sur vos systèmes
- Pas de fausses alertes
- Une recette de remédiation pour chaque alerte levée
- S'intègre à votre SIEM si vous le souhaitez

Pourquoi choisir CF-Sentinel ?

Les entreprises investissent du temps et des ressources significatives dans la sécurisation de leurs Assets – i.e. adresses IPs ou domaines - exposés à internet. Cependant, peu d'entre elles testent et valident régulièrement l'efficacité des contrôles de sécurité mis en place.

CF-Sentinel est une plate-forme de tests d'intrusions automatisés utilisant la méthodologie et les outils des cyber-attaquants. CF-Sentinel simule en continu ou à la demande des attaques permettant de tester la vulnérabilité d'une entreprise sans affecter le fonctionnement des systèmes évalués.

CF-Sentinel met en évidence les vulnérabilités de l'exposition digitale d'une organisation, afin de lui permettre de comprendre quelles tactiques, techniques et procédures d'attaque constituent une menace et, les accompagne dans la mise en place de mesures de sécurité délivrant une protection adéquate.

Comment fonctionne CF-Sentinel ?

CF-Sentinel recherche les informations sensibles accessibles en dehors de votre réseau et identifie les vulnérabilités qui ont un impact direct sur votre entreprise avant que quelqu'un d'autre ne le fasse.

CF-Sentinel surveille vos sites internet, DNS et IP ainsi que de nombreux autres services pour s'assurer que ceux-ci ne vous exposent pas à un risque : CUPS, DNS, HTTP/S, IMAP,

PREUVE DE CONCEPT

Si vous souhaitez réaliser un PoC, contactez-nous à poc@computablefacts.com

SITE WEB

Pour plus d'informations, consultez notre site web : https://computablefacts.com

KERBEROS, LDAP, MSSQL, MYSQL, ORACLE, POP3, RDP, SIP, SMB, SMTP, SNMP, SSH, TELNET, TFTP, VNC.

Une vulnérabilité est détectée. Et après ?

En cas de découverte d'une vulnérabilité, nous vous alertons aussitôt :

- Via un email si vous le souhaitez ;
- Via une alerte s'intégrant à votre SIEM.

Chaque alerte contient les informations nécessaires et suffisantes pour :

- Prioriser la prise en charge de l'alerte ;
- Identifier l'Asset concerné ;
- S'assurer de l'existence de la vulnérabilité ;
- Corriger la vulnérabilité ;
- S'assurer que la vulnérabilité a bien été corrigée.

Prix

- **Surveillance Asset Actif :** 20€ HT/mois/Asset
  (au moins un service exposé, dégressif selon volume à partir de 100 Assets)

- **Pack Surveillance 1000 Assets Passifs :** 10 000€ HT/an
  (surveillance passive de l'apparition de ports ou de services ouverts sans scans approfondis ni alertes)

- **Pack Surveillance 360° :** 10 000€ HT/an
  (leaks, pastes, mauvaise configuration de services Clouds, githubs)