INGRAM MICRO SECURITY

CATALOGUE OVERVIEW

Offensive Security Services

Contents

Introduction

Les cybermenaces continuent d'augmenter et toutes les entreprises et organisations, quels que soient leur taille, leur secteur ou leur localisation, sont ciblées par des cybercriminels du monde entier.

Nos services de sécurité offensive sont une approche proactive visant à protéger les systèmes informatiques, les réseaux et les appareils contre une cyberattaque, dans le seul objectif de minimiser l'impact de celle-ci et de protéger l'actif le plus précieux de votre entreprise, vos données.

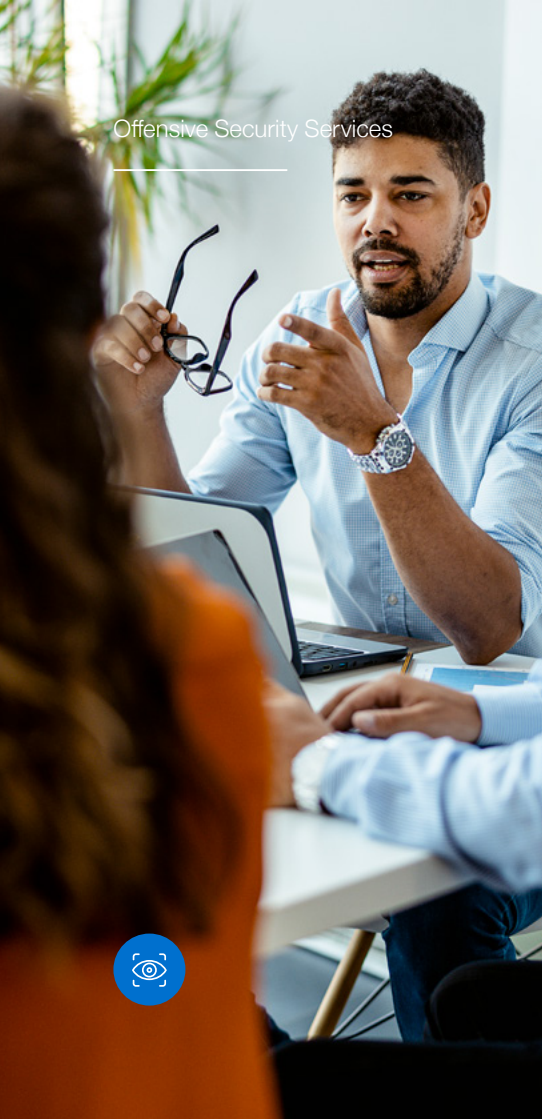
Service Process

Une fois le périmètre déterminé et un accord de confidentialité signé, nous effectuerons les démarches suivantes :

- **Règles et accord de collaboration**
- **Planification**
- **Exécution**
- **Post-exécution**
- **Évaluation post-remédiation**

Après l'analyse, un rapport sera délivré dans lequel nous étudierons les vulnérabilités détectées et les actions de remédiation possibles.

La méthodologie utilisée dans tous nos services est basée sur les normes de l'industrie.



EYESIGHT - Public Discovery Scan (libre)

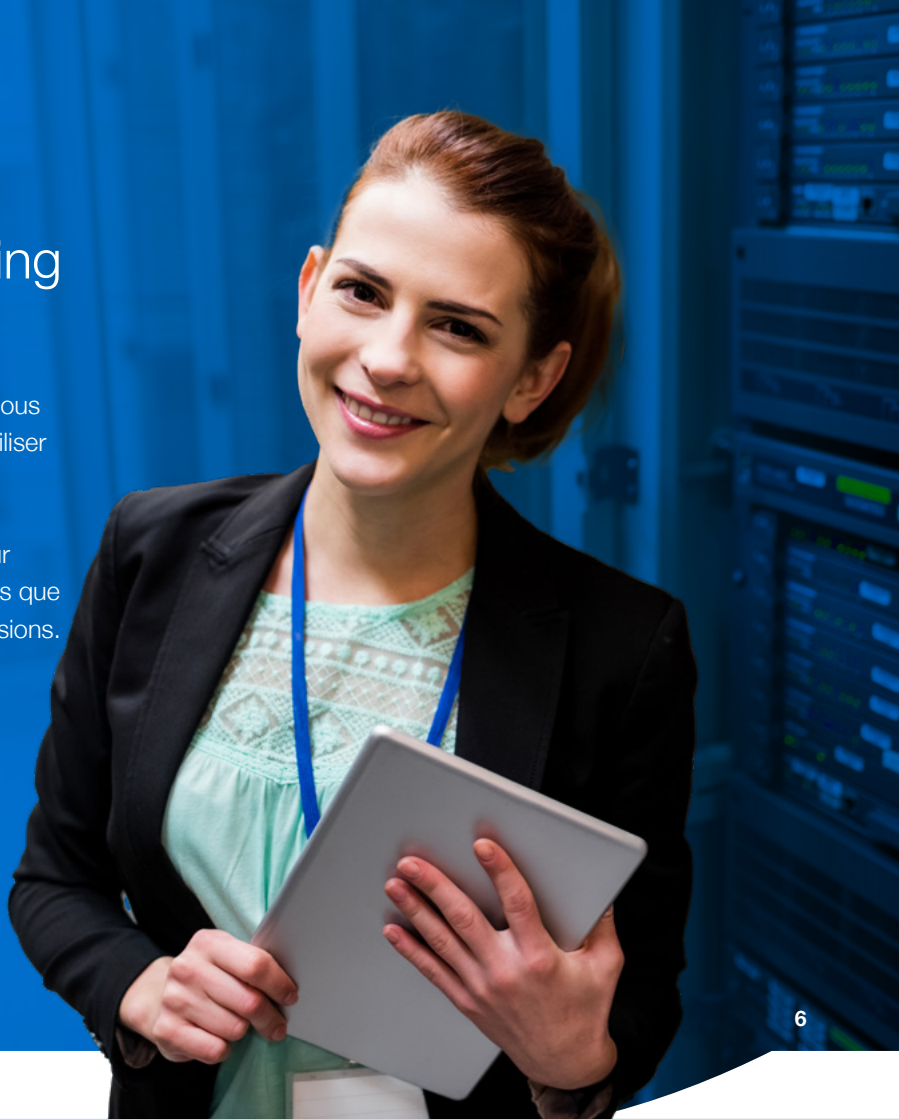
EYESIGHT est un service gratuit avec lequel nous aiderons les organisations à connaître le niveau de risque auquel elles sont exposées sur la base des informations publiques disponibles sur Internet de votre entreprise.

Ce n'est qu'avec le domaine de votre organisation que nous pourrons analyser les vulnérabilités de votre entreprise. Celles-ci sont visibles et accessibles à tous et, les robots des cyberattaquants traquent en permanence, étant à la base de toute attaque massive ou ciblée.

External Penetration Testing

L'objectif est de simuler une attaque provenant de l'extérieur de l'infrastructure. Il identifiera et évaluera tous les actifs exposés à Internet qu'un adversaire peut utiliser comme point d'entrée à son réseau d'entreprise.

Nous utilisons des outils automatisés et manuels pour valider l'efficacité de vos mécanismes de sécurité, tels que les pare-feux et les systèmes de prévention des intrusions.



Internal Penetration Testing

Simule une attaque effectuée depuis l'intérieur du périmètre de sécurité d'une organisation.

Son objectif est d'évaluer l'impact d'une attaque menée par un initié malveillant, tel qu'un employé mécontent. Le processus est toujours adapté aux besoins du client, mais il convient de noter qu'il implique généralement l'identification d'instances vulnérables et l'exfiltration d'informations critiques pour l'entreprise.

Evaluation of Active Directory

Les tests d'intrusion Active Directory (AD) dans un environnement Windows consistent à simuler les actions d'un attaquant ayant accès au réseau de l'entreprise. Cet accès peut être physique ou via un poste de travail infecté.

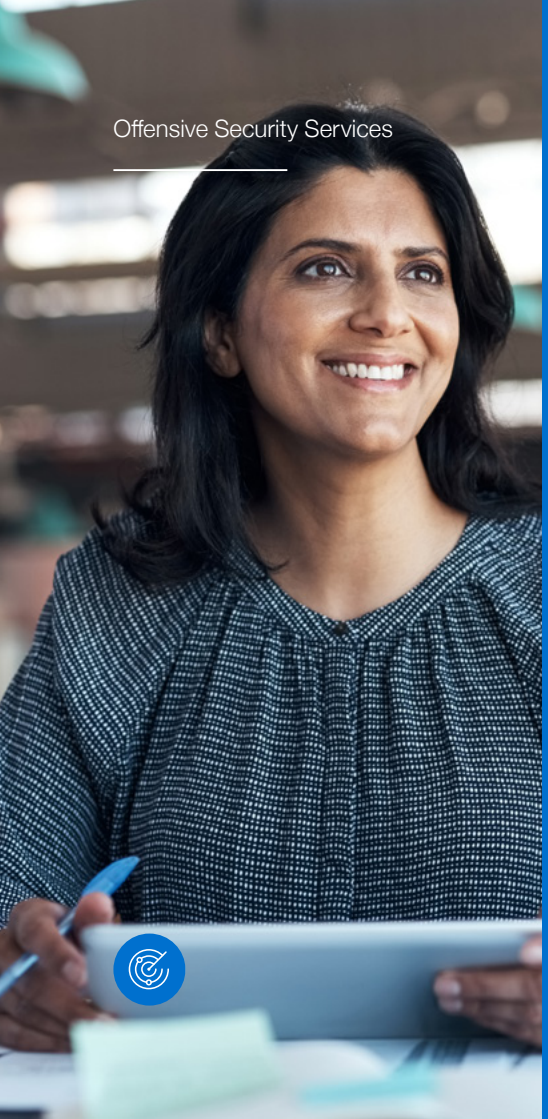
L'objectif principal est de trouver les actifs vulnérables qui affectent le périmètre de l'organisation et de proposer des plans d'action pour améliorer la posture de sécurité de l'AD.

L'objectif des tests Active Directory est d'identifier les problèmes de sécurité au sein du réseau interne d'une organisation.

Web Application Penetration Test

L'objectif des tests de pénétration des applications Web est d'évaluer la posture de sécurité des applications Web en identifiant et en examinant les vulnérabilités résultant de pratiques de conception et de mise en œuvre non sécurisées.

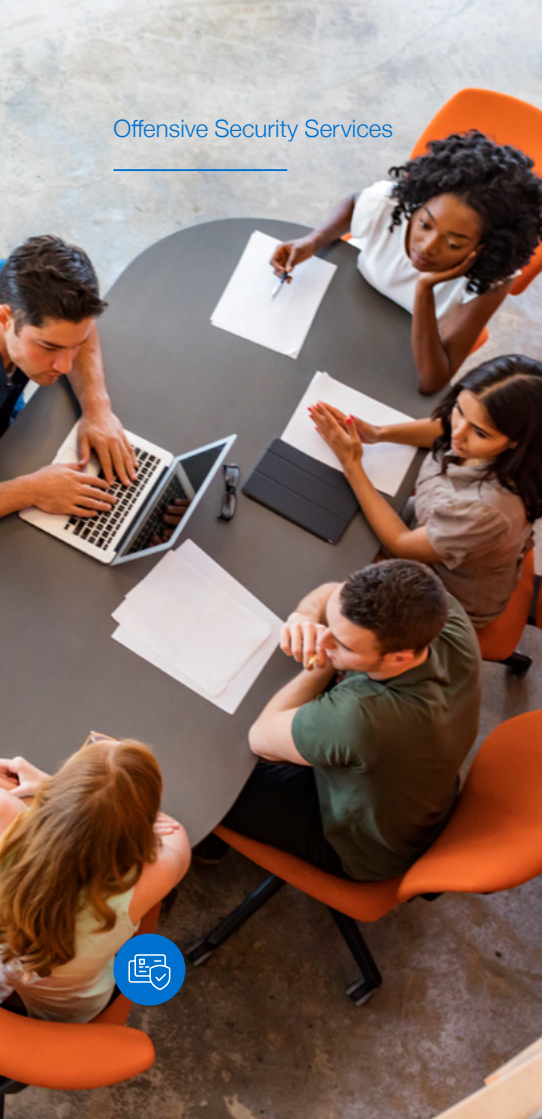
Elle est réalisée grâce à l'utilisation d'outils automatisés et manuels pour valider l'efficacité des mécanismes de sécurité, tels que le pare-feu applicatif Web WAF, par exemple.



API Penetration Test

Les tests de pénétration des interfaces de programmation d'applications (API) se concentrent sur l'évaluation de la posture de sécurité des environnements qui utilisent des API et nécessitent une transmission de données.

L'objectif est de modifier la logique de l'application et de provoquer l'exposition d'informations sensibles en accédant à des fonctionnalités et à des niveaux d'accès restreints. Les activités de test sont réalisées en utilisant principalement des manuels de techniques d'énumération et d'exploitation décrits dans le Guide de test de l'API OWASP.



Vulnerability Assessment

Les objectifs de l'évaluation des vulnérabilités sont d'identifier, de classer et de hiérarchiser les vulnérabilités dans les réseaux, les bases de données et les applications.

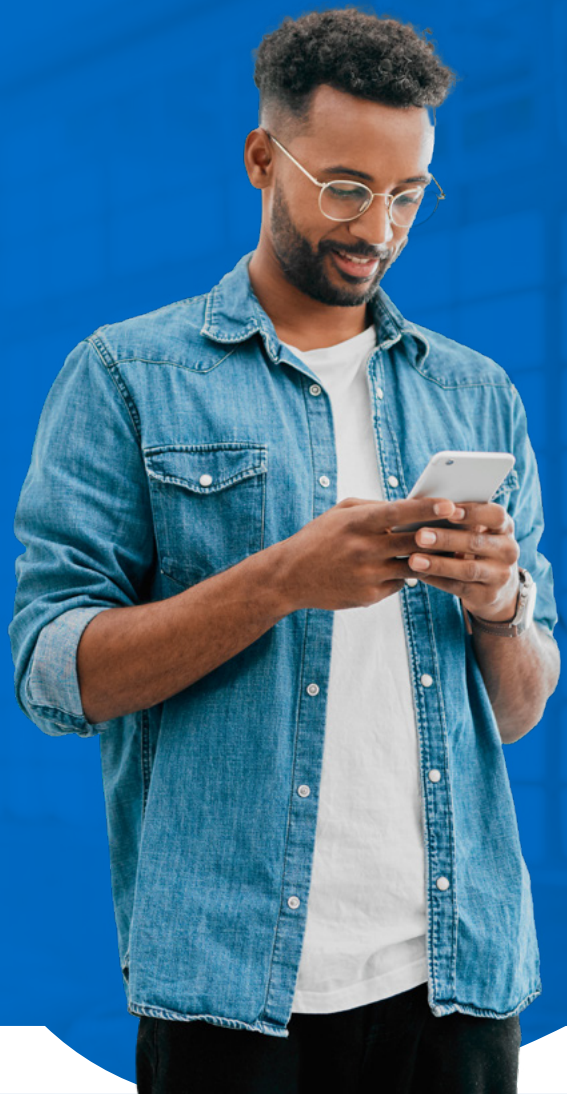
L'engagement est plus large et plus compliqué que les analyses courantes, car il implique également des politiques de test personnalisées pour détecter les violations et les erreurs de configuration des instances dans l'écosystème client. Grâce aux informations recueillies, les vulnérabilités sont classées et classées par ordre de priorité en fonction des meilleures pratiques du secteur en matière de gestion des risques. En ce qui concerne les types d'évaluations de la vulnérabilité, les engagements peuvent inclure :

- **Évaluations réseau et sans fil**
- **Évaluations de l'hôte**
- **Évaluations de la base de données**
- **Analyse des applications**

Mobile Application Penetration Test

L'objectif des tests de pénétration des applications mobiles est d'identifier les failles de sécurité dans les applications mobiles personnalisées sur les plates-formes Android et iOS.

Nous évaluons la sécurité d'une application par le biais d'analyses statiques et dynamiques en suivant les directives de test de l'Open Web Application Security Project (OWASP).



Cloud Environment Penetration Test

Les tests d'intrusion dans le cloud se concentrent sur les défauts de conception, de déploiement et de configuration dans les environnements hébergés dans le cloud.

Nos cyber-consultants utilisent un large éventail d'outils, de techniques et de procédures pour évaluer la posture d'une organisation d'un point de vue tant externe qu'interne.

Les mauvaises configurations et les politiques d'accès défectueuses ont joué un rôle majeur dans les récentes failles de sécurité. Ce que nous faisons, c'est aider nos clients à comprendre les risques et proposer des mesures d'atténuation pour un écosystème plus sûr.

Wi-Fi Penetration Testing

L'objectif du test d'intrusion Wi-Fi est d'identifier les failles de sécurité dans les implémentations actuelles du/des réseau(x) Wi-Fi.

Les tests de pénétration Wi-Fi peuvent également impliquer l'utilisation de l'ingénierie sociale, inciter les utilisateurs à révéler leur mot de passe Wi-Fi ou manipuler leur trafic sont des vecteurs d'attaque courants, et la plupart du temps avec un adaptateur réseau suffisamment puissant, peuvent être répliqués à partir du rue.

VoIP Penetration Testing

Voice over Internet Telephony Protocol (VoIP) est une technologie qui fournit des solutions de communication avancées et efficaces. La VoIP offre des fonctionnalités supplémentaires et, par conséquent, des vecteurs d'attaque supplémentaires. L'atténuation est essentielle pour renforcer davantage la posture de sécurité d'une organisation.

L'objectif du test d'intrusion VoIP est d'identifier les failles de sécurité dans la ou les implémentations actuelles de l'infrastructure VoIP.

Phishing Campaign Services

L'hameçonnage est une menace énorme et, de plus en plus répandu chaque année, il se classe au deuxième rang des causes les plus coûteuses de violation de données.

Ingram Micro propose des campagnes de phishing personnalisées menées par nos spécialistes du service pour tout type d'entreprise, indépendamment de la taille, du secteur ou des besoins spécifiques.

Cyber Security Assessment Tool (CSAT)

Créez votre plan d'action de cybersécurité en vous basant sur des faits. Votre compagnon pour la sécurité et la conformité (GDPR).

L'outil d'évaluation de la cybersécurité (CSAT) fournira rapidement aux équipes informatiques d'une organisation un aperçu des cyberrisques potentiels et les aidera à décider où et comment améliorer leurs mesures de sécurité.

CSAT analysera rapidement l'ensemble de l'infrastructure de l'entreprise, y compris les abonnements Microsoft 365 et Azure, à la recherche de vulnérabilités potentielles et de zones à risque afin de fournir des investissements intelligents et justifiés dans la sécurité, axés sur les faiblesses de l'organisation.

Cyber Threat Intelligence (OSINT)

Lors d'une évaluation des renseignements sur les cybermenaces, nos pirates éthiques certifiés traitent votre organisation comme leur cible et rassemblent les informations qu'ils utiliseraient pour lancer une attaque efficace.

Le type d'informations que nous recherchons lors d'une évaluation des menaces est le type qui pourrait être utilisé pour aider les attaquants à se faire passer pour un décideur de haut niveau, à lancer des cyberattaques plus efficaces, à lancer des campagnes d'ingénierie sociale et, par la suite, à compromettre votre sécurité. Ces informations sont utilisées pour préparer, prévenir et identifier les cybermenaces qui pourraient profiter de ces informations accessibles au public.

IoT Penetration Testing

Dans l'Internet moderne, les appareils Internet des objets (IoT) représentent un pourcentage croissant des appareils connectés à Internet, et avec l'essor de la 5G, l'IoT ne devrait que croître

Dans le test de pénétration de l'IoT, nous identifions les failles de sécurité causées par l'utilisation d'appareils IoT qui peuvent rendre le client vulnérable aux attaquants, en analysant et en testant l'ensemble de l'écosystème d'appareils IoT (du matériel au cloud) et en évaluant la posture de sécurité du client pour ce qui concerne l'IoT. L'objectif final est d'identifier avec précision les vulnérabilités et de calculer un score de risque global, en fournissant au client une vision globale et claire des chemins d'attaque, de l'impact possible, et de proposer des remédiations détaillées et personnalisées, afin de résoudre ou d'atténuer tous les problèmes. , protégeant au maximum le client.

INGRAM MICRO
SECURITY