INGRAM MICRO SECURITY

CATALOGUE OVERVIEW

Offensive Security Services

Contents

Introduction

Cybersecurity threats continue to increase and all companies and organizations, regardless of size, sector or location, are targeted by cybercriminals from all over the world.

Our Offensive Security services are a proactive approach aimed at protecting computer systems, networks, and devices against a cyber attack, with the sole objective of minimizing the impact of this and safeguarding your company's most valuable asset, your data.

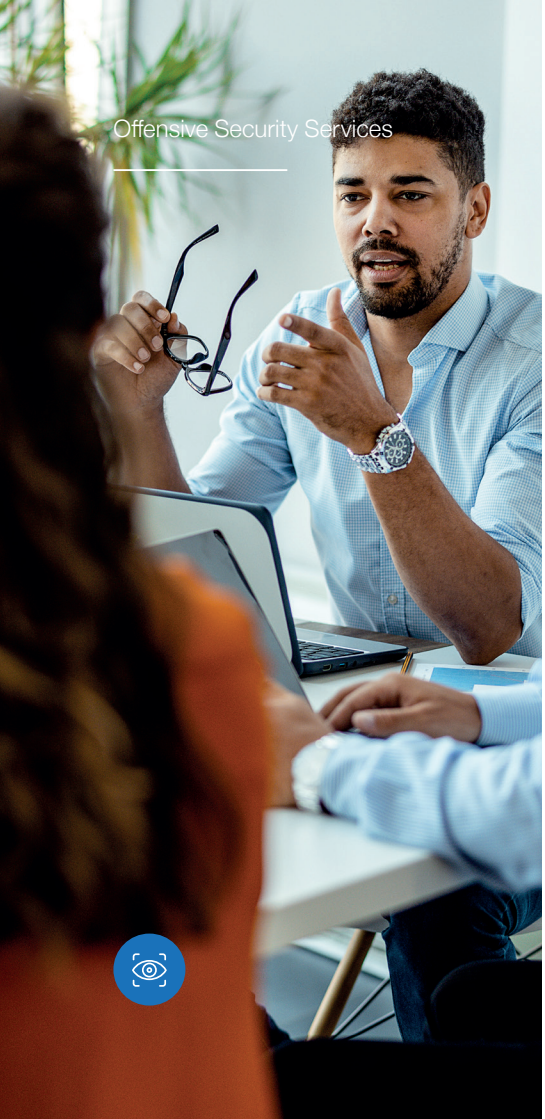
Service Process

Once the scope has been determined and a confidentiality agreement has been signed, we will carry out the following processes:

- **Rules and collaboration agreement**
- **Planning**
- **Execution**
- **Post-execution**
- **Post-remediation evaluation**

After the analysis, a report will be delivered in which we will study the vulnerabilities detected and possible remediation actions.

The methodology used in all our services is based on industry standards.



EYESIGHT - Public Discovery Scan (free)

EYESIGHT is a free service with which we will help organizations to know the level of risk to which they are exposed based on public information that is available on the Internet of your company.

Only with the domain of your organization will we be able to analyze the vulnerabilities of your company. These are visible and accessible to everyone and, the robots of cyberattackers continuously track, being the basis of any massive or targeted attack.

External Penetration Testing

The objective is to simulate an attack originating from outside the infrastructure. It will identify and evaluate all assets exposed to the Internet that an adversary can use as an entry point to its corporate network.

We use automated and manual tools to validate the effectiveness of your security mechanisms, such as firewalls and intrusion prevention systems.

Internal Penetration Testing

Simulates an attack carried out from within the security perimeter of an organization.

Its goal is to assess the impact of an attack carried out by a malicious insider, such as a disgruntled employee. The process is always tailored to the needs of the customer, but it should be noted that it usually involves the identification of vulnerable instances and the exfiltration of business-critical information.

Evaluation of Active Directory

Active Directory (AD) penetration testing in a Windows environment consists of simulating the actions of an attacker who has access to the corporate network. This access can be physical or through an infected workstation.

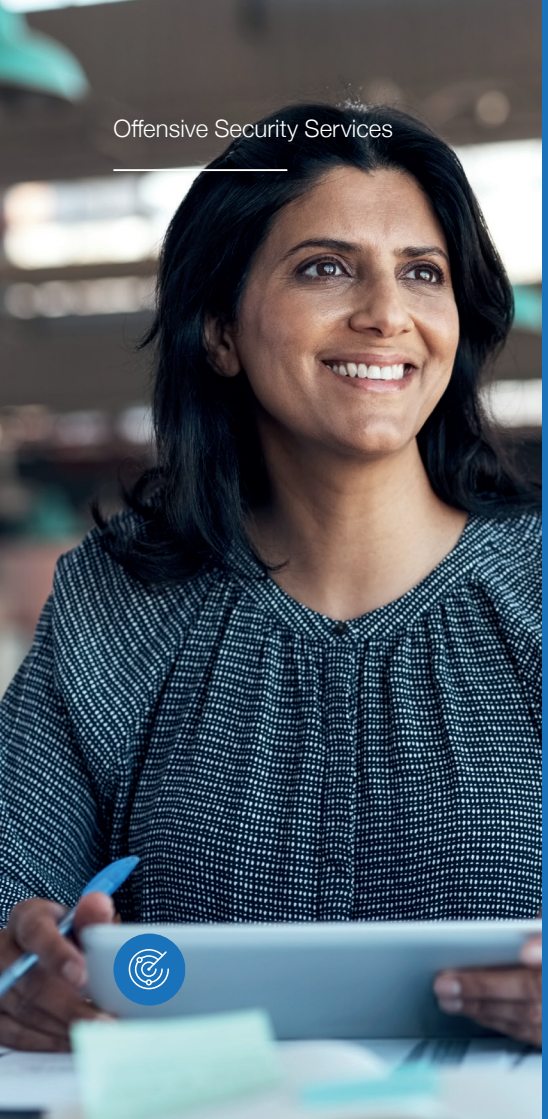
The main objective is to find vulnerable assets that affect the perimeter of the organization and propose action plans to improve the security posture of the AD.

The goal of Active Directory testing is to identify security issues within an organization's internal network.

Web Application Penetration Test

The goal of web application penetration testing is to assess the security posture of web applications by identifying and examining vulnerabilities resulting from insecure design and implementation practices.

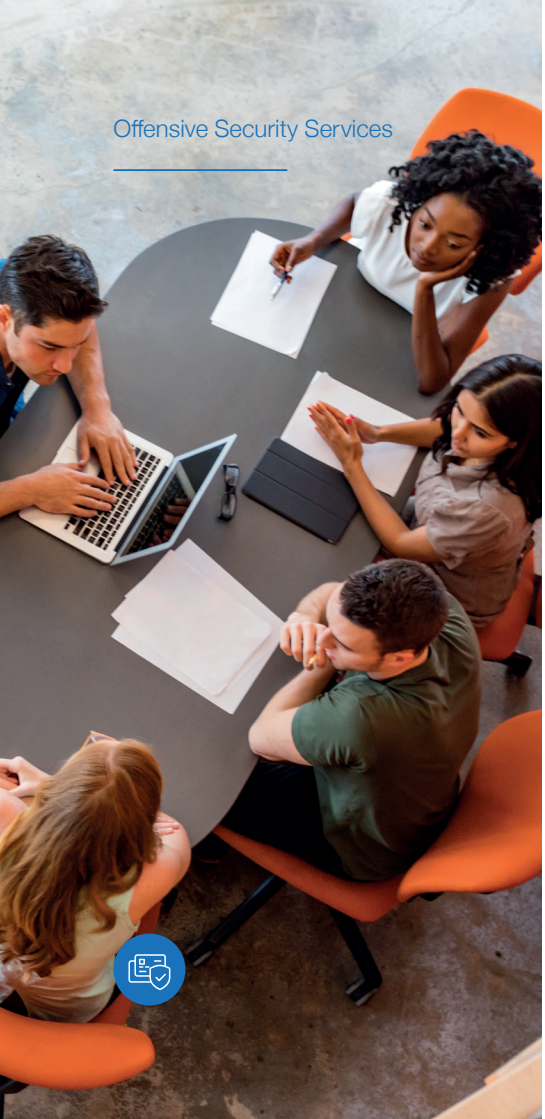
It is carried out through the use of automated and manual tools to validate the effectiveness of security mechanisms, such as web application firewall WAF, for example.



API Penetration Test

Application programming interfaces (APIs) penetration testing focuses on assessing the security posture of environments that use APIs and require data transmission.

The objective is to modify the logic of the application and cause exposure of sensitive information by accessing restricted functionalities and access levels. Testing activities are carried out using mainly enumeration and exploitation techniques manuals described in the OWASP API Testing Guide.



Vulnerability Assessment

The objectives of vulnerability assessment are to identify, classify and prioritize vulnerabilities in networks, databases, and applications.

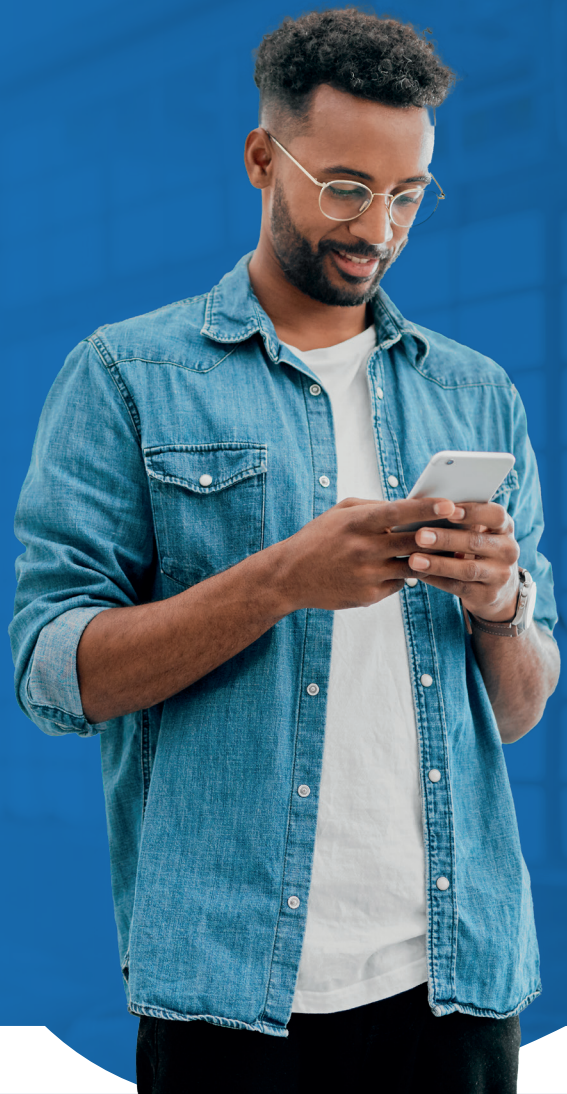
The commitment is broader and more complicated than common scans, as it also involves custom testing policies to detect breaches and misconfigurations of instances in the customer ecosystem. With the information gathered, vulnerabilities are classified and prioritized based on industry best practices for risk management. With respect to types of vulnerability assessments, commitments may include:

- **Network and wireless assessments**
- **Host Evaluations**
- **Database Evaluations**
- **Application Analysis**

Mobile Application Penetration Test

The goal of mobile app penetration testing is to identify security flaws in custom mobile apps on both Android and iOS platforms.

We evaluate the security of an application through both static and dynamic analysis following the test guidelines of the Open Web Application Security Project (OWASP).



Cloud Environment Penetration Test

Cloud penetration testing focuses on design, deployment, and configuration flaws in cloud-hosted environments.

Our cyber consultants use a wide range of tools, techniques, and procedures to assess an organization's posture from both an external and internal perspective.

Misconfigurations and flawed access policies have played a major role in recent security breaches. What we do is help our clients understand the risks and propose mitigation measures for a safer ecosystem.

Wi-Fi Penetration Testing

The objective of the Wi-Fi penetration test is to identify security flaws in the current Wi-Fi network/s implementations.

Wi-Fi penetration testing may also involve the use of social engineering, tricking the users into revealing their Wi-Fi password or manipulating their traffic are common attack vectors, and most of the time with a powerful enough network adapter, can be replicated from the street.

VoIP Penetration Testing

Voice over Internet Telephony Protocol (VoIP) is a technology that provides advanced and efficient communication solutions. VoIP offers extra functionality, and consequently, further attack vectors. Mitigation is essential to strengthen an organization's security posture further.

The objective of the VoIP penetration test is to identify security flaws in the current VoIP infrastructure implementation(s).

Phishing Campaign Services

Phishing is a huge threat and becoming more widespread every year, it ranks as the second most expensive cause of data breaches.

Ingram Micro offer customized phishing campaigns conducted by our service specialists for any type of company, independently of the size, sector, or specific needs.

Cyber Security Assessment Tool (CSAT)

Create your cybersecurity action plan base on facts. Your companion for Security & Compliance (GDPR).

The Cyber Security Assessment Tool (CSAT) will quickly provide the IT teams of an organization with an insight into potential cyber risks and help them decide where and how to improve their security measures.

CSAT will quickly scan an entire company infrastructure, including Microsoft 365 and Azure subscriptions, for potential vulnerabilities and risk areas in order to provide smart and justified investments in security that are focused on the organization's weaknesses.

Cyber Threat Intelligence (OSINT)

During a cyber threat intelligence assessment, our certified ethical hackers treat your organization as their target and gather the information that they would use to launch an effective attack.

The kind of information that we look for when performing a threat assessment is the kind that could be used to help attackers impersonate a high-level decision-maker, launch more effective cyber-attacks, initiate social engineering campaigns, and subsequently compromise your security. This information is used to prepare, prevent and identify cyber threats that might take advantage of this publicly available information.

IoT Penetration Testing

In the modern internet, Internet Of Things (IoT) devices make up a growing percentage of internet-connected devices, and with the rise of 5G the IoT is only expected to grow larger

In the IoT penetration test we identify the security flaws originated by the usage of IoT devices that may left the customer vulnerable to attackers, analysing and testing the entire IoT device(s) ecosystem (from hardware to cloud) and evaluating the customer security posture for what concern IoT. The final goal is to accurately identify the vulnerabilities and calculate an overall risk score, providing to the customer a global and clear vision of the attack paths, the possible impact, and suggest detailed and customized remediations, in order to fix or mitigate all the issues, protecting the customer as much as possible.


INGRAM MICRO
SECURITY
CERTIFIED RED TEAM PROFESSIONAL
CompTIA ISAO
Information Sharing and Analysis Organization
C|EH
Certified Ethical Hacker
OSCE
OSCP