Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

In collaboration with
CISCO

Cyber Security
Competence Service

Swascan Catalogue

Swascan.com
info@swascan.com

Come Piattaforma di
CyberSecurity in Cloud

Tra le 20 soluzioni
AL MONDO

Top 20 Cyber Security
firms in Europe

Cyber Security Research Team

Service Index

CSIRT

Swascan

4. Vulnerability Test

- Web Vulnerability Assessment
- Network Vulnerability Assessment

5. Phishing Attack Simulation

- Phishing Attack Simulation
- Human Risk Exposure

6. Penetration Test

- Penetration Test
- Pen Test Target

7. Domain Threat Intelligence

- Domain Threat Intelligence
- Osint & Closint

8. Cyber Threat Intelligence

- Data Breach
- Dark Web
- Network Hygiene
- Botnet Activity
- Various Risks

9. Code Review

- Standard Code Review
- Manual Code Review

10. Cyber Security Framework Checkup

- Cyber security framework Checkup

11. Consulting and training

- Cyber Security Consultancy
- Digital Forensic Analysis
- Training

12. GDPR, ISO & compliance

- GDPR Assessment
- ISO 27001 Assessment
- GDPR & ISO Consultancy
- Modalità Assistita

13. Swascan On Premise

- Swascan On Premise

14. Data Breach Incident Response Pack

- Identification
- Containment
- Sanitization
- Recovery
- Reporting

Mode

Self usage:

The Self usage mode provides the activity to be carried out by the customer.

Assited:

In the assisted mode, the services are carried out directly by Swascan personnel. This includes the activities of individual platform services and the examination of the reports produced.

Manual:

The activity involves the execution of the test in line with industry standards, using the proprietary platform and the skills of the Team. The activity includes: Information Gathering, Vulnerability Scan, Vulnerability Analysis, Reporting and Report discussion.

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

VULNERABILITY TEST

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

Web Vulnerability Assessment

Web App Scan is the automated service of Web Vulnerability Scan. The Vulnerability Assessment Scanner Tool allows you to identify vulnerabilities and security concerns of websites and web applications. The vulnerability analysis aims to quantify the levels of risk and indicates corrective and repositioning actions required for recovery

Network Vulnerability Assessment

Network Scan is the automated service of Network Vulnerability Scan. The online Network Scan service allows you to scan infrastructures and devices to identify vulnerabilities and security issues. The Vulnerability Analysis aims to quantify the levels of risk and to indicate the corrective actions and repositioning necessary for recovery.

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

PHISHING ATTACK SIMULATION

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

Phishing Attack Simulation

A dedicated, cloud-based Phisihing simulation attack platform that identifies the Human Factor risk and raises employee awareness consequently. The service allows you to identify your exposure to corporate phishing attacks and to educate your employees to recognize and identify malicious emails.

Human Risk Exposure

Human Risk Exposure makes it possible to determine human risk exposure in relation to potential social engineering activities. The activity is conducted through two activities:

- Social Engineering Threat Intelligence
- Phishing Attack Simulation

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

PENETRATION TEST

In collaboration with
CISCO

Cyber Security Research Team

Cyber Security
Competence Service

Penetration Test

Penetration Test is the service that aims to highlight any vulnerabilities and security issues present and to indicate technological, organizational and procedural countermeasures, able to eliminate vulnerabilities and problems, mitigate the effects and raise the overall security status of the entire technological infrastructure.

Pen Test Target

- Web sites
- Web applications
- Network
- Wifi
- IoT
- Mobile applications
- ATM
- Hardware

Pentest

Carries out the activity of Penetration test in both Black Box and White Box mode.

Vulnerability

Classifies vulnerabilities in terms of potential damage and impacts.

Reporting

Detailed documents regarding the activities carried out

Penetration Testing activities will be carried out taking into account the following reference methodologies:

- **OWASP Testing Guide**
- **Penetration Testing Execution Standard**
- **OSSTMM**

The following steps foreseen by the methodologies above will then be carried out:

- **Information Gathering**
- **Vulnerability Analysis**
- **Exploitation**
- **Post-Exploitation**
- **Reporting**

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

DOMAIN THREAT INTELLIGENCE

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

The **Domain Threat Intelligence** has the purpose and objective of identifying any public information available at OSINT and CLOSINT level relating to a given target. The activity of Threat Intelligence gathering is carried out through a process of research, identification and selection of publicly available information relating to the domain of interest.

Threat Intelligence

Threat Intelligence activity is carried out on targets and digital identifiers related to compromised assets and emails. The activity is conducted through the search, identification and selection of publicly available information relating to domain, subdomain and compromised email.

Osint & Closint

The service does not perform any security tests on the target, it operates only on information collected at the OSINT and CLOSINT level and available on the Dark Web.

OSINT: An acronym for Open Source Intelligence, it refers to the process of gathering information through the consultation of public domain sources also called "open sources" impacts.

CLOSINT: Close Source Intelligence, a process of gathering information through consultation of "closed sources", not accessible to the public or "reserved" areas.

Reporting

Detailed activity reports in PDF format.

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

CYBER THREAT INTELLIGENCE

In collaboration with
CISCO

Cyber Security Research Team

Cyber Security
Competence Service

Cyber Threat Intelligence represents the Intelligence capability developed in the field of Cyber Security. It includes the collection and analysis of information in order to characterize possible cyber threats from a technical point of view in relation to specific operational contexts.

Swascan's Cyber Threat Intelligence service has the purpose and objective to identify any public information available at OSINT and CLOSINT level related to a specific target. The activity includes the collection and analysis of information related to a series of critical macro areas such as:

Data Breach

Data Breach detected (direct and/or third party) and compromised emails. Depending on the case you can provide:

- Password used
- Password Hash
- Record without password, but of which there is trace in the Deep and Dark Web

Dark Web

Analysis of instances on the so-called Dark Web, such as threat actors (cyber criminals, typically) on cyber crime forums who have spoken about the Client (understood as brands, domains, IP addresses, brands or names of Executives) to spread confidential or personal data, to discuss scams and fraud to be perpetrated against the Client, etc..

Various Risks

This category of digital risk includes several subcategories: Ip Reputation (see below), DNS Passive, etc. The impacts vary depending on the type of information that is present outside the Client's business perimeter.

Network Hygiene

Identifies the presence of malicious or suspicious activity within the Client's digital perimeter. Depending on the type of evidence found, the keyword can be associated, for example, to the "IP Reputation", i.e. the reputation of certain IP addresses, known worldwide and the various cyber security communities and anti-virus companies, for having carried out illegal activities, or to indirectly facilitate such activities (due to configuration and/or implementation errors), with all the legal consequences (civil and criminal) of the case.

Botnet Activity

A botnet is a network of computers infected with malware, spyware, key loggers, etc. The "bot hardener" (the botnet manager) can use its botnet network to launch attacks (e.g. DDoS), or instruct it to steal credentials (e-banking, corporate intranet, civil and criminal legal liability, information theft, industrial espionage, etc.).

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

CODE REVIEW

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

Code Review Standard

Secure Code Review is the automated **Static Code Analysis service**. The service allows to identify, analyze and solve security problems and vulnerabilities of the source code. It provides an action plan and a remediation plan.

Standard language :

- Android
- Csharp
- Groovy
- Java
- Javascript
- Php
- Python
- Web
- ABAP
- C/C++
- C#
- COBOL
- iOS
- Objective-C
- PL/SQL
- RPG
- VB.NET
- Visual Basic 6

Code Review Manual

The Manual Code Review service is provided by Swascan's Code Review experts. The activity involves the analysis of the evidence of vulnerability or criticality identified during the automated analysis phase (Code Review Base and/or Code Review Premium) in order to identify and eliminate any false positives.

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

CYBER SECURITY FRAMEWORK CHECKUP

In collaboration with
CISCO

Cyber Security Research Team

Cyber Security
Competence Service

Cyber Security Framework Checkup

The Cyber Security Framework Checkup activity is divided in 5 separate steps:

Mapping

Obj

- Elencare gli asset aziendali
- Identificare gli asset e strumenti di Security
- Determinare i sistemi di alert ed Early Warning dei Security Asset
- Analizzare i processi e le metodologie di gestione

Actions

- Asset Inventory
- Software Inventory
- Information Gathering tramite interviste
- Analisi dei Security Asset

Output

- Executive Summary
- Report Asset Inventory
- Report Software Inventory
- Report Security Asset

Assess Threats

Obj

- Identificare le vulnerabilità e criticità
- Definire i livelli di severity delle vulnerabilità
- Valutare la probabilità di utilizzo delle vulnerabilità
- Calcolare il livello di rischio al netto delle misure di sicurezza

Actions

- Vulnerability Assessment
- Network Scan
- IT Security Assessmernt
- Penetration Test
- Phishing Simulation Attack

Output

- Executive Summary
- Technical Executive Report
- Technical Report

Security KPI

Obj

- Determinare i Security KPI in uso
- Identificare i Security KPI applicabili
- Valutare i Security KPI da adottare

Actions

- Analisi gestione sistemi di allarm e early warning
- Analisi security KPI in uso
- Analisi Security Policy e procedure

Output

- Executive Summary
- Technical Report

Gap Analysis

Obj

- La GAP Analysis permette di determinare e confrontare lo stato attuale (as-is) del Cyber Security Framework rispetto alle best practice di settore, normative e obiettivi interni

Actions

- Analisi dello stato attuale (AS-IS)
- Evidenza delle criticità
- Definizione modello a tendere (TO-BE)
- Gap Analysis

Output

- Executive Summary
- Report Assessment

Security Road Map

Obj

- Percorso dettagliato di riposizionamento dell'attuale Cyber Security Framework, una sequenza temporale di azioni attraverso la quale ci si aspetta di raggiungere l'obiettivo.

Actions

- Definizioni e piano a livello organizzativo
- Definizioni e piano a livello Policy e Procedure
- Definizioni e piano a livello Tecnologico
- Definizioni e piano a livello competenze e know how

Output

- Report Action Plan in base alle priorità:
  High
  Medium
  Low

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

CONSULTING AND TRAINING

In collaboration with
CISCO

Cyber Security Research Team

Cyber Security
Competence Service

Cyber Security Consultancy

Cyber Security Consultancy is the Swascan MSSP service provided by experienced Cyber Security Professionals through a daily consulting activity. It plays an advisory and operations role to support the customer in order to: define the security policies of the information systems, assess risks, control and supervise the entire technological infrastructure of the company. Specifically, the service allows you to enstablish a:

Digital Forensic Analysis

It's the consulting service to support businesses. Forensic computing is a branch of digital forensic science linked to the evidence acquired by computers and other digital storage devices. Its purpose is to examine digital devices following forensic analysis processes in order to identify, preserve, retrieve, analyze and present facts or opinions regarding the information collected. It is a necessary support in case of Data Breach, computer fraud or abusive access to the computer system.

Training

Cyber Security Training are tailor-made training and awareness courses related to the world of Cyber Security. The courses are managed and recognized professionals in the field. The courses are delivered according to the customer's needs, according to the needs with the aim of being in line with the technological context of the company. Below is the list of courses:

Cyber Security Course:

- Ict Security Awareness
- Governance, Risk and Compliance
- Incident & Crisis Management
- Ethical Hacking
- Secure Coding
- Strumenti e Tecnologie
- .....

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

GDPR, ISO & COMPLIANCE

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

GDPR Assessment

GDPR Assessment is the online tool that allows companies to verify and measure their level of compliance according to the legislative provision on privacy, the General Data Protection Regulation - EU Regulation 2016/679. The Swascan GDPR service provides guidance and corrective actions to be taken at the level of Organization, Policy, Personnel, Technology and Control Systems.

ISO 27001 Assessment

ISO 27001 Assessment is the online tool that allows companies to verify and measure their level of compliance with the international standard ISO. It provides the indications and corrective actions to be taken to set up and manage the information security management system (SGSI or ISMS), in terms of logical, physical and organizational security.

GDPR & ISO Consultancy

GDPR and ISO Consultancy is Swascan's MSSP service provided by experienced professionals from the fields of GDPR, ISO and Compliance through a daily consulting activity. It plays an advisory and operational role in supporting the client in order to identify technological and process solutions for regulatory and legislative compliance.

Assisted Mode

Assisted Mode allows companies to be supported by Swascan's staff in the execution of individual services. The activity includes:

- Additional manual activities related to the selected service
- Execution of the selected service
- Manual verification of false positives of individual reports
- Discussion of the Report remotely
- Indication of remediation plans

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

SWASCAN ON PREMISE

In collaboration with
CISCO

Swascan's Platform

Cyber Security
Competence Service

Swascan On Premise

Cyber Security Training are tailor-made training and awareness courses related to the world of Cyber Security. The courses are managed and recognized professionals in the field. The courses are delivered according to the customer's needs, according to the needs with the aim of being in line with the technological context of the company. Below is the list of courses

On Premise

Installing the Swascan platform on a local server or private infrastructure.

Cyber Security Testing

Carries out security testing of the company's technological assets at the level of applications, software and devices.

Technologic Risk Assessment

It guarantees the Analysis of Technological Risk (GDPR art.32) and the management of Security Governance.

Compliance

Verification of conformity with the regulations in force. It provides an analysis of risk levels together with indications for the resolution of vulnerabilities.

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

DATA BREACH INCIDENT & RESPONSE PACK

In collaboration with
CISCO

Cyber Security Research Team

Cyber Security
Competence Service

Identification

- Identify attack vectors
- Determine the entry point of the attack
- Establish the target victims of the attack
- Specify the technique and methodology used

Containment

- Identify vulnerabilities and critical issues
- Define the severity of vulnerabilities found
- Assessing the likelihood of exploit of said vulnerabilities

Sanitization

- Eliminate the key and triggering components of the incident.

Recovery

- Determine the effectiveness of the previous remediation plan through a Gap Analysis
- Measure Security Key Performance Indicator

Reporting

- Production of Data Breach Incident REsponse process related documents

Swascan.com
info@swascan.com

Swascan

The First Cyber Security Testing Platform

Cloud *or* ***On Premise*** *Platform*

In collaboration with
CISCO

Cyber Security
Competence Service

Swascan Catalogue

Swascan.com
info@swascan.com

Come Piattaforma di
CyberSecurity in Cloud

Tra le 20 soluzioni
AL MONDO

Top 20 Cyber Security
firms in Europe