
CYBERSECURITY & DIGITAL INTELLIGENCE

Digital Protection for Companies.

We think like an attacker. We work so you are prepared beforehand.

◆ Pentest

◆ Vulnerabilities

◆ OSINT

◆ AppSec

◆ Forensic

◆ Response

► WHO WE ARE

Cybersecurity with real focus.

At SAD Technological Solutions we help identify vulnerabilities, information exposure and digital risks before they can become real incidents.

We combine offensive cybersecurity, forensic analysis and digital intelligence to evaluate the attack surface of an organization, validate risks and establish concrete protection measures.

Our goal is not to generate hundreds of technical alerts: it is to identify what represents a real risk, what its impact could be and what must be corrected first.



Penetration Testing · Ethical Hacking

OFFENSIVE SECURITY

Controlled simulation of attack techniques on previously authorized systems to identify exploitable vulnerabilities in applications, networks and infrastructure.



Vulnerabilities Analysis

TECHNICAL EVALUATION

Identification and prioritization of vulnerabilities, insecure configurations, exposed services, outdated software and other weak points that increase the attack surface.



OSINT & Digital Intelligence

DIGITAL INTELLIGENCE

Investigation and analysis of publicly available information to identify digital exposure: domains, subdomains, infrastructure, known leaks and digital footprint.



Web Application & API Security

APPLICATION SECURITY

Technical evaluation of applications and APIs to identify authentication, authorization, configuration, information exposure and other security vulnerabilities.

▸ SERVICES

More protection capabilities.



Digital Forensic Analysis

FORENSIC & EVIDENCE

Preservation and technical analysis of digital evidence related to security incidents, unauthorized access, information leaks and possible system compromises.



Incident Response

INCIDENT RESPONSE

Technical support to identify the origin and scope of an incident, contain the threat, preserve evidence and establish corrective actions to reduce the risk of recurrence.



Security Audit

SECURITY AUDIT

Evaluation of infrastructure, access controls, configurations and security practices to detect gaps and opportunities for strengthening.

▸ CORPORATE INVESTIGATION

Beyond cybersecurity.

We combine digital intelligence, forensic analysis and investigation methodology to support organizations facing internal irregularities, third-party risks or legal processes that require solid technical evidence.



Internal Fraud and Irregularities

INTERNAL INVESTIGATION

Identification and analysis of irregular behavior, unauthorized access, manipulation of information or improper use of resources. We combine digital forensic analysis with review of logs, systems and user activity to document findings with technical evidence.



Due Diligence of Partners, Suppliers and Counterparties

THIRD PARTY INTELLIGENCE

Investigation of digital backgrounds, reputation, corporate links, public exposure and risk signals of individuals or organizations before establishing a commercial, contractual or investment relationship.



Internal Investigations

AUDIT & INVESTIGATION

Technical support for internal investigation processes in case of suspicions of improper conduct, conflicts of interest, confidential information leaks or policy non-compliance. Preservation of digital evidence with chain of custody.

▸ CORPORATE INVESTIGATION

Analysis, evidence and legal support.



OSINT and Third Party Risk

OPEN SOURCE INTELLIGENCE

Collection and analysis of publicly available information to evaluate the digital profile, online footprint and possible risks: domains, infrastructure, known leaks, networks and digital presence.



Reconstruction of Facts and Evidence

APPLIED FORENSIC ANALYSIS

Technical analysis to reconstruct event chronologies, identify actors involved and document what happened, when and from where. Applicable to incidents, commercial disputes, unauthorized access and information loss.



Technical and Documentary Support for Legal Matters

EXPERTISE & LITIGATION

Preparation of expert technical reports, opinions and documentation of digital evidence oriented to legal processes, arbitrations or requirements of authorities. Written in clear technical-legal language for legal teams.

► OUR METHODOLOGY

Structured process, concrete results.

01

Reconnaissance

We identify assets, technologies, services and attack surface within the authorized scope.

02

Discovery

We analyze possible vulnerabilities, insecure configurations and attack vectors.

03

Validation

We verify findings to distinguish real vulnerabilities from false positives.

04

Risk Analysis

We evaluate how different weaknesses could be combined and what their potential impact would be.

05

Technical Report

We document evidence, severity, impact and specific remediation recommendations.

06

Retest

After implementing the corrections, we verify that the vulnerabilities have been mitigated.

► DELIVERABLES

Clear documentation for all levels.

Each assessment can include an Executive Report directed at business leaders and a Technical Report for remediation teams.

- ✓ Executive Summary
- ✓ Technical findings and evidence
- ✓ Classification and prioritization of risks
- ✓ Priority action plan
- ✓ Potential Impact
- ✓ Identified scenarios and attack routes
- ✓ Remediation recommendations
- ✓ Subsequent validation of corrections



DO NOT WAIT TO DISCOVER A VULNERABILITY

when someone else has already exploited it.

We think like an attacker. We work so you are prepared beforehand.



sad.org.mx



contact@sad.org.mx

SAD Technological Solutions, S.A. de C.V.

CYBERSECURITY · DIGITAL INTELLIGENCE · INVESTIGATION · FORENSIC ANALYSIS

CONFIDENTIAL · EXCLUSIVE USE OF THE CLIENT · All evaluations are performed exclusively on expressly authorized systems, under a previously agreed scope and within the applicable legal framework.