iSec

FOR OVER 19 YEARS

CYBERSECURITY SERVICE PROVIDER

LICENSED

NTRA

National Telecom Regulatory Authority

الجهاز القومي لتنظيم الإتصالات

CERTIFIED

ISO

27001

REGISTERED

الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

Cyber Security
Services Provider

Governance, Risk & Compliance · Red Team · Blue Team

Compliance you can defend. Attacks you can simulate. Defenses you can prove.

SAMA | NCA | CBE | FRA | MITRE ATT&CK | ISO 27001 | PCI DSS

Cairo · Riyadh

ABOUT ISEC GROUP

One partner for compliance, offense, and defense

iSec Group is one of the leading cybersecurity companies in MENA, protecting organizations across the financial sector, government, fintech, oil & gas, utilities, and FMCG. Founded and chaired by Dr. Bahaa Eldin M. Hasan — a cryptography pioneer whose career spans smart-card security patents and two decades teaching security across the Arab world — iSec pairs regulatory fluency, offensive tradecraft, and real-world defensive operations under one roof, from Cairo and Riyadh.

INDUSTRIES WE SERVE

- Banking & Finance
- Government
- Fintech
- Oil & Gas
- Utilities
- FMCG

19
years of offensive, defensive & compliance experience

2
offices — Cairo & Riyadh, covering KSA and Egypt

47
services across three disciplines: GRC, Red Team, Blue Team

100+
certified security experts

6+
regulated industries served across MENA

5
regulators we work under: SAMA, NCA, DGA, CBE, and FRA

Our Mission

Resilient digital ecosystems through advanced cybersecurity expertise, strategic protection, and continuous innovation.

Our Vision

To become the benchmark for cybersecurity excellence, shaping a safer and more secure digital world.

WHY ISEC GROUP

Four reasons clients choose us

Three disciplines, one partner

GRC, Red Team, and Blue Team sit in the same practice — compliance findings, attack simulations, and detection tuning inform each other, instead of three vendors passing reports back and forth.

Always framework-current

Assessments track the versions regulators and adversaries actually use — PCI DSS v4.0.1, ISO/IEC 27001:2022, NCA ECC-2:2024, MITRE ATT&CK — so findings map to today's requirements and threats.

Practitioners, not theorists

Our consultants come from technical security roots — architecture, exploit development, SOC operations — so recommendations are implementable, not generic checklists.

End-to-end, assess to sustain

One practice takes you from gap analysis or Red Team simulation through implementation, certification, detection, and ongoing operation — including outsourced roles like vCISO.

OUR PRACTICE

Three disciplines, one security partner

Governance, Risk & Compliance

Board-ready compliance, risk, and privacy programs across two of the region's toughest regulatory environments.

28 SERVICES · SIX PRACTICE AREAS

Red Team

Real-world adversary simulation across applications, infrastructure, cloud, and specialized industry systems.

15 SERVICES · FOUR SPECIALISMS

Blue Team

Detection, incident response, and forensics that prove your controls actually catch what Red Team throws at them.

4 SERVICES · TWO SPECIALISMS

---

47 services across three disciplines and eight practice areas — one partner from first gap analysis to sustained defense.

PART ONE

Governance, Risk & Compliance

Compliance you can defend. Risk you can see. A partner regulators recognize.

OUR GRC PORTFOLIO

28 services across six practice areas

Regulatory Compliance

KSA, Egypt & FRA mandates

Standards & Certification

ISO · PCI DSS · SOC 2 · NIST

Risk Management

Enterprise & third-party risk

Data Privacy & Protection

PDPL · Law 151/2020 · DPO

GRC Strategy & Transformation

Operating models · platforms · vCISO

Security Architecture & Technical Reviews

Design & configuration assurance

PRACTICE AREA 01

Regulatory Compliance — Saudi Arabia & Egypt

SAMA Cybersecurity Framework Assessment	Maturity measurement across all SAMA CSF domains, with a prioritized remediation roadmap for regulator reporting cycles.
NCA ECC Compliance Assessment (ECC-2:2024)	Controls assessment against the current Essential Cybersecurity Controls, closing gaps before audit.
NCA CCC / OTCC / DCC Assessments	Cloud, operational technology, and data control assessments for organizations in scope of NCA's extended framework
CBE Cybersecurity Framework Assessment	Alignment assessment for banks and payment providers regulated by the Central Bank of Egypt.
FRA Cybersecurity Framework Assessment	Alignment assessment for capital market firms, insurers, and non-bank financial institutions regulated by Egypt's Financial Regulatory Authority.
SWIFT CSP Independent Assessment	Independent CSCF assessment supporting the annual attestation mandatory for SWIFT-connected institutions.
National & Sector Mandate Assessments	Compliance evaluations against additional national cybersecurity mandates applicable to your sector and market.

Who needs this: banks, insurers, and non-bank financial firms under SAMA, CBE, or FRA supervision; government and critical-infrastructure entities under NCA mandates; any SWIFT-connected institution.

PRACTICE AREA 02

Standards & Certification Readiness

ISO/IEC 27001 Information Security Management	Gap analysis through certifiable ISMS implementation — risk methodology, SoA, policies, and internal audit — with support through the certification audit itself.
ISO/IEC 20000 IT Service Management	Implement and certify an ISO/IEC 20000-1 service management system that aligns IT service delivery with business needs and international best practice.
Other ISO Standards	Gap analysis, implementation, and certification support across further ISO management standards — including ISO 9001 quality and ISO/IEC 42001 AI management.
PCI DSS v4.0.1	From gap analysis to full implementation — scoping, segmentation, compensating controls, and evidence readiness — with a clear path to your ROC or SAQ.
ISO 22301 Business Continuity	A certifiable BCMS that keeps critical operations running through disruption — an increasing regulatory expectation.
SOC 2 Readiness Assessment	Preparation for SOC 2 Type I/II mapped to the Trust Services Criteria — essential for tech providers selling to enterprises.
NIST CSF 2.0 Alignment	A board-ready maturity baseline that maps cleanly onto SAMA and NCA requirements.

Certification is a journey we finish with you: gap analysis → implementation → pre-audit → audit-day support → surveillance readiness.

PRACTICE AREAS 03 · 04

Risk Management & Technical Security Reviews

RISK MANAGEMENT

Cybersecurity Risk Assessment	Identify, analyze, and prioritize cyber risks using ISO 27005 / NIST methodology — delivering a risk register and treatment plan leadership can act on.
Threat Modelling	Map realistic attack paths against critical systems and applications before adversaries do, prioritizing defenses where they reduce the most risk.
Third-Party & Vendor Risk Management	Tiering, due-diligence assessments, contractual controls, and continuous monitoring — satisfying SAMA and NCA third-party requirements.

SECURITY ARCHITECTURE & TECHNICAL REVIEWS

Security Architecture Review	Evaluate network, cloud, and application architectures against best practice and regulatory expectations — finding design weaknesses before they become incidents.
Configuration Review	Assess system, network, and cloud configurations against CIS and vendor hardening benchmarks, with a prioritized remediation list.
MITRE ATT&CK Assessment	Map your detection and defence coverage against MITRE ATT&CK adversary tactics and techniques — revealing blind spots and prioritizing the controls that close them.

PRACTICE AREAS 05 · 06

Data Privacy & Protection & GRC Strategy

DATA PRIVACY & PROTECTION

Data Privacy & Protection Assessment	How personal data is collected, processed, stored, and shared — with a gap report against the laws that apply to you.
Saudi PDPL Compliance	Records of processing, privacy notices, consent, cross-border transfer rules, and breach procedures under the Saudi PDPL.
Egypt Data Protection Law (151/2020)	Licensing, DPO appointment, and data-subject rights handling under Egypt's data protection law.
Policy & Procedure Development	A complete, framework-aligned policy suite tailored to your organization — not templates.

GRC STRATEGY & TRANSFORMATION

GRC Transformation	Redesigned operating models — roles, processes, metrics, reporting — giving leadership one view of risk and compliance.
GRC Software Implementation	Selection, configuration, and rollout of the right GRC platform, with adoption support that makes it stick.
Virtual CISO (vCISO)	Senior security leadership on demand: strategy, board reporting, regulator liaison, and program oversight.

PART TWO

Red Team & Blue Team

Attacks you can simulate. Threats you can catch. Defenses you can prove.

OUR RED & BLUE TEAM PORTFOLIO

19 services across two disciplines, six specialisms

Application & API Security

Web · API · Mobile · Thick client · Source code

Infrastructure, Cloud & Wireless

Network · Active Directory · Wireless · Cloud

Specialized & Industry Systems

OT/ICS · Telecom · POS · ATM/ITM

Human Risk & Vulnerability

Phishing assessment · Vulnerability assessment

Detection & Incident Response

Compromise assessment · Incident response

Assurance & Forensics

Configuration review · Forensic services

Red Team (15 services) · Blue Team (4 services)

PRACTICE AREA 01 · RED TEAM

Application & API Security Testing

Web App Pentest	Identify and remediate security vulnerabilities in web applications, authentication systems, APIs, and business logic.
API Pentest	Assess API security by identifying vulnerabilities in authentication, authorization, endpoints, and data handling.
Mobile App Pentest	Secure Android and iOS applications against data leaks, insecure storage, and authentication weaknesses.
Thick Client Pentest	Detect security flaws in desktop applications, client-server communication, and local data storage.
Source Code Review	Analyze source code to identify security flaws, insecure coding practices, and logic vulnerabilities.

Every engagement ends with a proof-of-exploit walkthrough, a severity-ranked findings report, and a remediation retest.

PRACTICE AREA 02 · RED TEAM

Infrastructure, Cloud & Wireless Testing

Network Pentest	Evaluate internal and external network security to identify exploitable vulnerabilities and misconfigurations.
Active Directory Pentest	Identify privilege escalation paths, weak policies, and domain security misconfigurations.
Wireless Pentest	Evaluate Wi-Fi and wireless network security against unauthorized access and wireless attacks.
Cloud Pentest	Identify security weaknesses in cloud environments, configurations, and cloud-hosted applications.

From perimeter to Active Directory to the cloud control plane — the paths a real attacker would actually take.

PRACTICE AREAS 03 · 04 · RED TEAM

Specialized Systems & Human Risk & Vulnerability

SPECIALIZED & INDUSTRY SYSTEMS

OT/ICS Pentest	Identify vulnerabilities in operational technology and industrial control systems to improve resilience.
Telecom Pentest	Assess telecom infrastructure, communication protocols, and network security against cyber threats.
POS Pentest	Secure Point-of-Sale systems against payment fraud, malware, and unauthorized access risks.
ATM/ITM Pentest	Assess ATM and ITM systems for vulnerabilities in software, networks, and transaction security.

HUMAN RISK & VULNERABILITY

Phishing Assessment	Evaluate employee awareness and organizational resilience against phishing and social engineering attacks.
Vulnerability Assessment	Discover and prioritize security vulnerabilities across applications, networks, and systems.

Why these two pair together: technical breadth (industrial, telecom, payment systems) and human-layer risk are the attack surfaces standard pentests skip.

PRACTICE AREAS 05 · 06 · BLUE TEAM

Detection & Incident Response & Assurance & Forensics

DETECTION & INCIDENT RESPONSE

Compromise Assessment	Identify hidden threats and indicators of compromise, detect breaches, assess risk, and improve organizational resilience.
Incident Response Services	Rapidly contain, investigate, and remediate cyber incidents to minimize business disruption and accelerate recovery.

ASSURANCE & FORENSICS

Configuration Review	Assess security configurations across systems, networks, and applications to identify weaknesses and reduce risk.
Forensic Services	Investigate cybersecurity incidents, uncover attack origins, and collect digital evidence to support recovery, compliance, and legal requirements.

Blue Team validates whether the controls your policies describe actually detect and stop the attacks your Red Team simulates.

HOW WE WORK

One journey, from first gap to sustained security

1

Assess & Simulate

Gap analysis, risk assessment, or Red Team adversary simulation — benchmarked against your regulatory frameworks and real-world threat activity.

BOARD-READY FINDINGS REPORT

→

2

Remediate & Respond

Implementation of controls, policies, and platforms, paired with Blue Team detection and incident response — engineered, not just documented.

CLOSED FINDINGS, HARDENED SYSTEMS

→

3

Certify & Validate

Certification and attestation support, alongside retesting that proves controls actually stop what they're designed to stop.

CERTIFICATION / ATTESTATION

→

4

Sustain

Ongoing operation through vCISO, DPO-as-a-Service, continuous monitoring, and threat hunting — compliance and defense that hold over time.

COMPLIANCE & DEFENSE THAT HOLD

Engagements can enter at any stage — many clients start with a single assessment and grow into a multi-year partnership across GRC, Red Team, and Blue Team.

WHAT WE OFFER

Solutions iSec Can Provide

Threat & Vulnerability Mgmt

PICUS, tenable one

Network Security

Opinnate, TITANIA

Identity & Access Mgmt

sectona, segura, Delinea

Application Security

ThreatModeler

Malware Analysis & File Security

VMRAY, glasswall

Data Protection / DLP

SECLORE, DATAPATROL

Security Operations (SOC/SIEM/SOAR/XDR)

ANOMALI, imperum, Fidelis Security

Training & Simulation

SimSpace

AI Security & Governance

ACALVIO AI-POWERED DECEPTION, Quilr

Cloud & Container Security

sysdig

Phishing / Email Security

dPhish

GRC

جذور ETHUR

Cryptography / Key Mgmt

utimaco

Browser & Remote Access

MENLO SECURITY

OT / IoT / IoMT Security

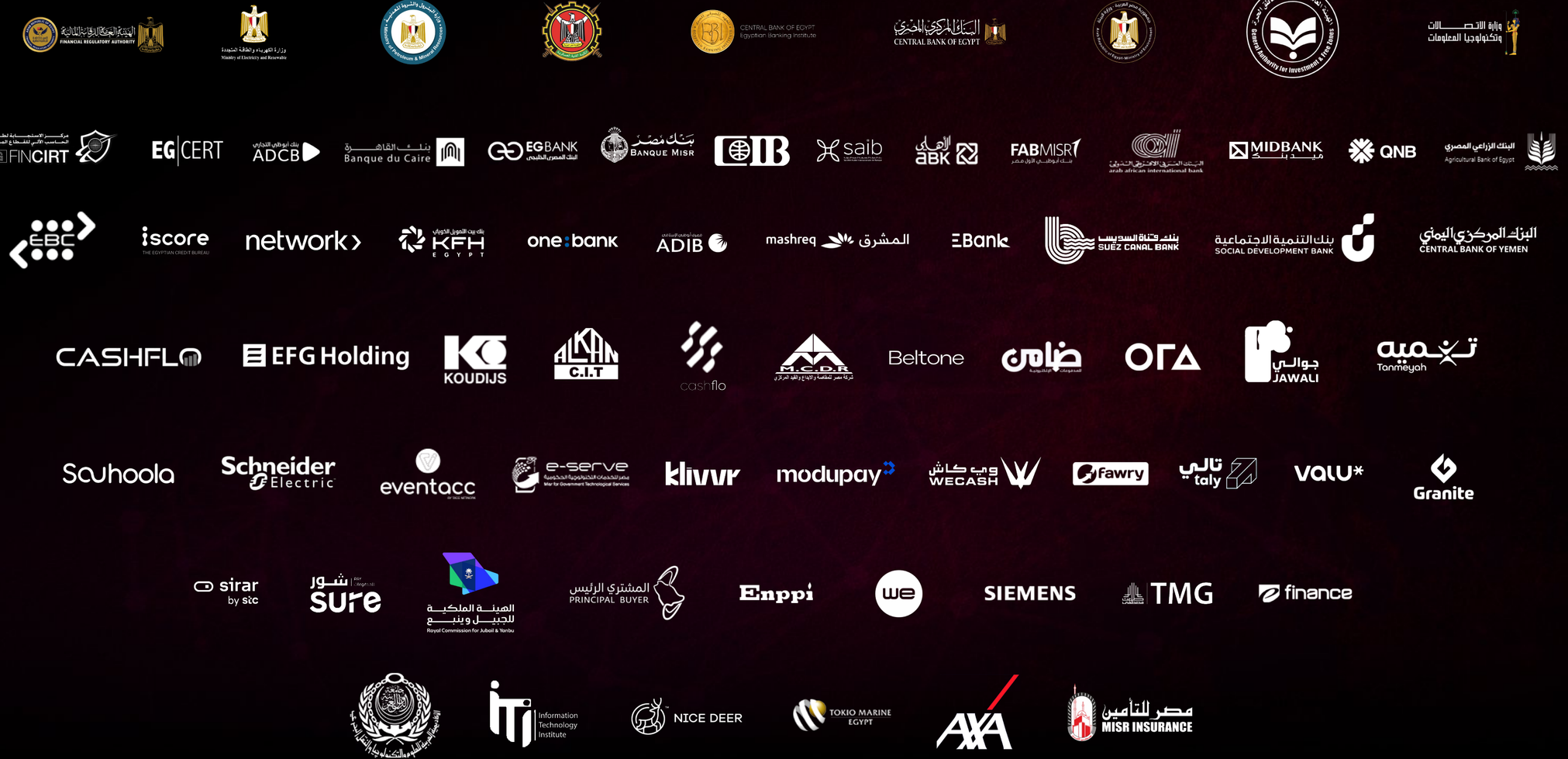
asimily

CREDENTIALS

iSec Certification Arsenal

TRACK RECORD

Success Stories & Client References



Egypt’s First NTRA-Licensed Cybersecurity Service Provider

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الاتصالات

شهادة تسجيل

شركة / اي سيك للبرمجيات وحماية المعلومات I SEC

كمقدم لخدمات الأمن السيبراني في جمهورية مصر العربية

(مستوى أول)

لخدمات

١. اختبارات الاختراق (Penetration Testing)
٢. خدمات الفريق الأحمر (Red Teaming)
٣. خدمات تقييم الثغرات الأمنية (Vulnerability Assessment)
٤. خدمات الحلول المتكاملة والاستشارية
٥. خدمات التدريب

م/ محمد شمروخ

الرئيس التنفيذي
للجهاز القومي لتنظيم الاتصالات

رقم الشهادة: CSP-2025050001

تاريخ الإصدار: 19 /5 /2025
تاريخ الانتهاء: 18 /5 /2028

ISEC GROUP

Let's talk about your security & compliance roadmap

Start with a readiness conversation — GRC, Red Team, Blue Team, or all three.

Cairo

41 Zaker Hussein, 5th Floor Nasr City, Cairo, Egypt

Riyadh

Akaria Plaza, Gate D, 6th Floor Olaya Street, Riyadh, KSA

Get in touch

info@isec-group.com isec-group.com