iSec

CYBER SECURITY
SERVICE PROVIDER

Company
Profile & Services

www.iSec.com.eg

Table of Content

About iSec	1
Mission, Vision and Value	2
About ASC Group	3-4
iSec Services	5-8
Our Team	9
Our Reputation	10
Our Clients	11
Our Courses	12-14

About iSec

As a Cyber Security provider, we provide Cyber Security services and solutions to establish a consistent and secure environment within companies handling confidential data. Our Firm was launched in May 2015 with cyber security market experience since 2007 and cyber security personal experience since 1980.

iSec is one of MENA's leading cybersecurity companies, providing cybersecurity services and solutions to the Financial, Oil and Gas ,Public, and Private Sectors.

At iSec, we place great emphasis on the following values as the building blocks of our success: confidentiality, innovation, integrity, quality, competency, efficiency, integrated solutions, and responsibility. These values are fundamental to our approach and underpin our commitment to delivering exceptional service and driving meaningful impact in the field of cybersecurity.

Our Mission, Vision, and Value

Mission:

advance the provision of cybersecurity services and solutions to create a secure and reliable environment for entities entrusted with confidential data. We specifically target financial service providers who face significant challenges in Securing customers' information, including credit/ debit card details and other personal data, with a focus on ensuring that quality-based standards are maintained.

Vision:

To establish ourselves as the preeminent cybersecurity company in Egypt and the wider Middle East region.

Value:

- Confidentiality
- Innovation
- Integrity
- Quality
- Competency
- Efficiency
- Integrated
- Solutions
- Responsibility

About ASC Group

Range of Services

We provide professional cyber security services below

Penetration Testing
- Mobile Application Pentest
- Web Application Pentest
- Network Pentest
- ITM&ATM Pentest
- Wireless Pentest
- ICS/SCADA Pentest
- Voice over IP (VoIP)
- POS Pentest
- Red Teaming
- Vulnerability Assessment

GRC Services
- Governance
- Risk Assessment
- Compliance
- ISO 27001 Implementation
- PCI-DSS Implementation
- ISO & PCI-DSS Gap Analysis
- Configuration Review
- GRC Transformation

Other Services
- Code Review
- Identity and Access Security
- Cyber Security Talents Hiring
- Threat Intelligence Feeds
- Configuration Management Database (CMDB)
- Brand and Reputation Management
- Data classification
- Deep Packet Inspection (DPI)
- A Threat Intelligence Platform (TIP)
- Privileged Access Management (PAM)

We are system integrator and resellers for the below vendors

iSec Services

Penetration Testing

Mobile Application Pentest

Mobile application penetration testing attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. it's a critical component in any comprehensive security plan, after web applications, more concern area is mobile application penetration testing.

Web Application Pentest

Web application penetration testing is the process of using penetration testing techniques on a web application to detect its vulnerabilities. It aims to break into the web application using any penetration attacks or threats. it works by using manual or automated penetration tests to identify any vulnerability, security flaws, or threats in a web application. The tests involve using / implementing any of the known malicious penetration attacks on the application.

Red Teaming

Red Teaming is a full-scope, multi-layered attack simulation designed to measure how well a company's people networks, applications, and physical security controls can withstand an attack from a real-life adversary. Red teaming helps a business remain competitive while securing its business interests by leveraging social engineering and physical, application, and network penetration testing to find ways to shore up your defenses.

Network Pentest

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. Network penetration testing is a Network Security Service, which is one of several methods used to prevent unauthorized network intrusion. Network Pentest involves a variety of methodologies designed to explore a network to identify potential vulnerabilities and test to ensure the vulnerabilities are real.

ITM&ATM Pentest

is a specialized security assessment focused on evaluating the security of ITMs (Information Technology Machines) and ATMs (Automated Teller Machines). This type of assessment is crucial for financial institutions and organizations that operate these machines. The purpose of an ITM&ATM Pentest is to identify vulnerabilities and weaknesses in the systems to ensure the security and confidentiality of financial transactions and customer data.

Wireless Pentest

A Wireless Penetration test is an authorized hacking attempt, which is designed to detect and exploit vulnerabilities in security controls employed by a number of wireless technologies and standards, misconfigured access points, and weak security protocols.

Vulnerability Assessment

A systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

ICS/SCADA Pentest

This service aims at Penetration Testing of the SCADA network and services configured at the different components of the HMI, RTUs, and Controller Machine. The communication protocols used by the applications are also inspected against the industry standards. The tests are operated by skilled certified consultants without causing any possible downtime to the environment.

Voice over IP (VoIP)

is a technology that allows the transmission of voice and multimedia content over Internet Protocol (IP) networks. Instead of using traditional circuit-switched networks, VoIP uses packet-switched networks to send voice data. This technology is widely used for making phone calls over the internet and within organizations to streamline communication.

POS Pentest

is a specialized security assessment aimed at evaluating the security of a Point of Sale system. This type of assessment is crucial for businesses that handle financial transactions and utilize POS systems. a POS Pentest aims to identify vulnerabilities and weaknesses within the POS system and associated infrastructure to ensure the security and confidentiality of sensitive payment card data.

GRC Services

Governance

Establishes a structured framework aligning security with business goals and compliance. It includes defining roles, policies, and procedures to manage risks and maintain a robust security posture. against NIST, ISO, CBE regulation, GDPR, and PCI-DSS...etc. The goal is to protect data, ensure compliance, and promote a security-oriented culture.

Risk Assessment

A cyber security risk assessment identifies the information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property). It then identifies the risks that could affect those assets.

Compliance

compliance management to safeguard data and maintain operational integrity within the framework of information security. This approach helps in establishing a robust security posture, mitigating threats, and demonstrating a commitment to regulatory requirements.

ISO 27001 Implementation

An international standard that sets out the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) within an organization. The standard provides a systematic and structured approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. By implementing ISO 27001, organizations can enhance the protection of their information assets, reduce the risk of security breaches and data leaks, gain customer trust, and demonstrate their commitment to information security best practices.

PCI-DSS Implementation

It is a set of security requirements developed by the Payment Card Industry Security Standards Council (PCI SSC) to ensure the secure handling of credit card information. The standard applies to any organization that processes, stores or transmits cardholder data, including merchants, financial institutions, and service providers. Compliance with PCI DSS helps organizations protect cardholder data, reduce the risk of data breaches and fraud, and build customer trust. It is important for organizations to understand and implement the requirements of PCI DSS to ensure the security of payment card information and maintain compliance with industry standards.

ISO & PCI-DSS Gap Analysis

A gap analysis is a process that helps organizations identify the gaps or differences between their current state and a desired state or specific requirements, such as those outlined in ISO standards or PCI DSS. Both ISO and PCI gap analyses are conducted to assess an organization's compliance with the respective standards and identify areas that need improvement.

Configuration Review

Hardening network devices reduces the risk of Unauthorized access to a network's infrastructure. Vulnerabilities in device management and configurations present weaknesses for a malicious cyber actor to exploit in order to gain presence and maintain persistence within a network. Adversaries have shifted their focus from exclusively exploiting traditional endpoints to increasingly exploiting specialized and embedded devices, including routers, switches, and firewalls. They do this through manipulating weaknesses in configurations, controlling routing protocols, and implanting malware in the operating systems.

GRC Transformation

iSec has been working in the Security field for many years therefore we would support the organizations managing Security GRC operations with automation solution that facilitates Risk Management, Compliance Management, Policy Reviews, Internal Control Testing, Online Assessments, Reminders, and Reports. Through this transformation, the GRC team will be able to manage, follow up, Assess, and audit Documentation and processes related to Governance, Risk, and Compliance. All these aspects connected to each other on the same platform would ease initializing any project and assessment by the GRC management team. We will help implement a tool that is built and distributed as a simpleand cheap alternative to GRC spreadsheets and scattered folders. Eramba charges only to operate (supporting and administration). So as a huge or small organization, Eramba would be an affordable tool for all Organizations seeking GRC management in an easy, professional, and sufficient manner.

Other Services

Code Review

A secure code review is a specialized task involving manual and / or automated review of an application's source code in an attempt to identify security -related weaknesses (flaws) in the code. A secure code review does not attempt to identify every issue in the code but instead looks to provide insight into what types of problems exist and to help the developers of the application understand what classes of issues are present. The goal is to arm the developers with information to help them make the application's source code more sound and secure.

Identity and Access Security

Our daily life has become interlaced with fast-evolving technology from e-government to e-commerce and more. This growth has not spared the corporate world, but it frequently targets it specifically. For example, remotely accessing an enterprise's resources or financial transactions causes threats to individual users and organizations. Consequently, the need for secure and reliable web access has become very important. iSec provides a solution to make web access more secure and fend off credentials hacking. Our Solution includes two alternatives, which are PKI-based Secure Web Access and OTP-based Secure Web Access.

Threat Intelligence Feeds

refer to streams of information regarding potential and current cyber threats and vulnerabilities. These feeds are collected from a variety of sources to provide organizations with insights and data to help them understand and mitigate potential risks to their information systems and infrastructure.

Cyber Security Talents Hiring

we are responsible for hiring the cyber security team which is more than 100 employees in the Central Bank of Egypt and financial cert.

Configuration Management Database (CMDB)

is a centralized repository that holds information about the configuration items (CIs) within an organization's IT infrastructure. It's a fundamental tool used in IT service management (ITSM) and ITIL (Information Technology Infrastructure Library) practices to manage and track configuration items and their relationships.

Brand and Reputation Management

involves actively monitoring, shaping, and influencing the public perception of a brand or organization to maintain a positive i mage and foster trust among stakeholders.

Data classification

Is a systematic process of organizing and categorizing data based on its sensitivity, value, or importance to an organization. This process helps in efficiently managing and protecting data according to its specific requirements for confidentiality, integrity, and availability.

Deep Packet Inspection (DPI)

Is a technology used in network security and traffic analysis to inspect and analyze the contents of data packets traversing a network. Unlike traditional packet inspection, which only examines packet headers, DPI dives deep into the payload or data portion of each packet to extract detailed information about the traffic and its content.

A Threat Intelligence Platform (TIP)

is a comprehensive software solution designed to collect, aggregate, analyze, and manage threat intelligence data from various sources. TIPs assist organizations in understanding the threat landscape, identifying potential risks, and making informed decisions to enhance their cybersecurity posture.

Privileged Access Management (PAM)

is a cybersecurity strategy and set of technologies that focuses on controlling and securing access to critical systems, applications, and data by privileged users or accounts within an organization. Privileged users typically have elevated access rights and permissions, granting them the ability to perform critical actions, make significant changes, and access sensitive information within an organization's IT environment.

Our Team

We have trusted and competent talents who are highly skilled in discovering vulnerabilities and conducting penetration testing based on industry standards and customized in-house built methodologies. Throughout the years, our consultants have executed many projects and achieved exceptional results, in which zero days were discovered and many bugs were hunted. Our team is always up to date with the latest ethical hacking techniques, and are actively updating our methodologies to cope with new threats.

Our Reputation

Research-oriented assessment We depend on manual tests to identify unknown vulnerabilities that might exist in target systems such as zero-day vulnerabilities. Therefore, we facilitate research capabilities for the security experts to utilize throughout the projects and for skills development.

High-quality services We adopt quality assurance processes to offer high-quality services. The quality of our services is supported by demonstrable capabilities with effective and proven security assessment methodologies that are tailored for each environment type.

World-renowned security researchers Our world-renowned security experts are qualified and competent in their areas of specialization. The passion is behind the determination of iSec security consultants to always produce results that make us proud of what we do.

Our Clients

Our Courses

Computer Hacking Forensic Investigator Certification v10

EC-Council's Certified Hacking Forensic Investigator (CHFI) is the only comprehensive ANSI accredited, lab-focused program in the market that gives organizations vendor-neutral training in digital forensics. CHFI provides its attendees with a firm grasp of digital forensics, presenting a detailed and methodological approach to digital forensics and evidence analysis that also pivots around Dark Web, IoT, and Cloud Forensics. The tools and techniques covered in this program will prepare the learner for conducting digital investigations using ground-breaking digital forensics technologies. The program is designed for IT professionals involved with information system security, computer forensics, and incident response. It will help fortify the application knowledge in digital forensics for forensic analysts, cybercrime investigators, cyber defense forensic analysts, incident responders, information technology auditors, malware analysts, security consultants, and chief security officers. The program equips candidates with the necessary skills to proactively investigate complex security threats, allowing them to investigate, record, and report cybercrimes to prevent future attacks.

The Certified Penetration Testing Professional (CPENT)

EC-Council's Certified Penetration Tester (CPENT) program teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended

Certified Network Defender Certification v2

Learn the skills that matter! EC-Council's vendor-neutral network security certifications provide an unbiased approach to learning secure networking practices, as well as how to analyze and harden computing systems prevalent in the current IT infrastructure. CND v2 has earned a reputation as the only program in the market that is 100% focused on network security and defense. IT professionals need to be part of the cybersecurity ecosystem, especially in a post-COVID Digital Transformation era. If you think cybersecurity is the responsibility of cyber teams alone, think again! Certified Network Defender v2 has been designed by industry experts to help IT Professionals play an active role in the Protection of digital business assets and Detection and Response to Cyber Threats, while leveraging Threat Intelligence to Predict them before they happen. CND is a network security course designed to help organizations create and deploy the most comprehensive network defense system. CND is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE).

Certified Threat Intelligence Analyst (C|TIA

The Certified Threat Intelligence Analyst (CTIA) program is designed and developed in collaborationwith cybersecurity and threat intelligence experts across the globe. The aim is to help organizations hire qualified cyber intelligence-trained professionals to identify and mitigate business risks by converting unknown internal and external threats into quantifiable threat entities and stopping them in their tracks. Much like a 'hunter-killer' team, you'll be deployed as a 'Blue Team' operative, tasked with threat identification, and asked to employ the tools at hand to thwart active and potential cyberattacks.

Certified Ethical Hacker Certification v12

The C|EH v12 program helps you develop real-world experience in ethical hacking through the hands-on C|EH practice environment. C|EH Engage equips you with the skills to prove that you have what it takes to be a great ethical hacker.

ICS/SCADA Cybersecurity

Industrial automation processes use industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems to control industrial processes locally or remotely and to monitor, gather, and process real-time data. As the rapid growth of interconnectivity among systems continues (i.e., Internet of Things, Industrial Internet), ICS and SCADA systems are now accessible and becoming high-priority targets for hackers. Cybercriminals have already developed malware threats that can disrupt industrial Operation Technology (OT). Due to the potential impact of an attack on the physical safety of communities, employees, or customers, ICS/SCADA security is an even higher priority than traditional IT systems.

Certified Application Security Engineer (CASE)

The CASE-certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application. Unlike other application security training, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, and testers globally, and respected by hiring authorities.

EC-Council's Certified Chief Information Security Officer

The CCISO Certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security.

THANK YOU

www.iSec.com.eg