CYBER SECURITY:

SERVIZI PER CREARE UNA CULTURA DIGITALE A TUTELA DEL BUSINESS AZIENDALE

IMQ group

CONTRO LE MINACCE INFORMATICHE

CYBER SECURITY

#VULNERABILITÀ #DIFESA

IMQ group

CYBER SECURITY: UNA QUESTIONE DI CULTURA E MATURITÀ

Gli incidenti di sicurezza stanno crescendo molto rapidamente, sia nel numero sia nella loro efficacia.

Questo problema risulta sempre più rilevante, e lo sarà ancora di più in futuro, in quanto il processo in atto di Digital Transformation della società è ormai inarrestabile. In particolare, le aziende hanno capito che per rimanere in vita, crescere e diversificare, devono considerare la tecnologia digitale come parte integrante dei propri processi, prodotti e servizi. Mentre risultano chiari i benefici di tale cambiamento, **manca la consapevolezza sulle vulnerabilità create da questa trasformazione,** vulnerabilità che molto spesso risultano difficili da riconoscere e da intercettare, perché il perimetro non è più solamente tecnologico. C'è quindi la necessità di verificare, monitorare e rendere sicuro l'intero ecosistema, di qualcosa che vada al di là della sola tecnologia.

È quindi fondamentale affrontare il tema della sicurezza informatica in tutti i suoi aspetti, focalizzandosi su tutti gli elementi che compongono un'azienda: **infrastruttura, software, persone e cultura aziendale.**

L'obiettivo del Gruppo IMQ è di rendere consapevoli le aziende dei rischi che possono scaturire dall'insieme di queste vulnerabilità ed aiutarle a porvi rimedio.

La proposizione del Gruppo IMQ sulla Cyber Security si fonda sui seguenti pilastri:

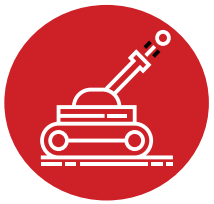
I PILASTRI PER UNA CULTURA DIGITALE	**ASSESSMENT**	**DEFENSE**
VERIFICATION & ACCREDITED VERIFICATION	**OPERATIONS**	**CERTIFICATION**

ASSESSMENT

#ORGANIZZAZIONE #TECNOLOGIA
#FATTORE UMANO

ASSESSMENT
QUANTO È SICURA LA TUA AZIENDA?

VALUTAZIONI TECNICHE PER MISURARE IL LIVELLO DI SICUREZZA DELLA TUA ORGANIZZAZIONE, DELLA TUA AZIENDA, DEI TUOI SOFTWARE, IN TERMINI DI PROCESSI, STANDARD E TECNOLOGIE IN USO



RED TEAM

Servizio per dimostrare se e come sia possibile creare un danno di business alle aziende. Simulando un vero attacco informatico, il servizio Red Team aiuta l'azienda a verificare se la strategia di sicurezza adottata è efficace nel contrastare anche gli attacchi di ultima generazione che possano creare un danno di business. Utilizzando mentalità e tecniche offensive reali, il servizio viene svolto guardando le aziende con gli occhi di un "hacker", di un vero attaccante che, non disponendo di alcuna informazione da parte dell'azienda, cerca le vulnerabilità più critiche - tecnologiche e/o umane - e le usa per raggiungere il proprio scopo.
L'azienda che aderisce a una iniziativa Red Team ha la possibilità di dare uno sguardo al futuro per comprendere ciò che potrebbe accadere.

COMPANY SECURITY ASSESSMENT

Servizio che consente di ottenere una valutazione sul livello di maturità dell'azienda nei confronti della sicurezza informatica, evidenziando le principali carenze nella protezione dei dati personali rispetto a quanto prescritto dalla normativa UE 2016/679 (GDPR). Sulla base delle informazioni che vengono fornite dal cliente, il servizio - sviluppato secondo alcuni framework consolidati (CIS, NIST) - evidenzia le carenze aziendali riconducibili a una gestione inadeguata, a problemi di natura tecnologica o alla mancanza di una condivisa cultura della sicurezza aziendale.

SOFTWARE SECURITY ASSESSMENT

Servizio basato su analisi di sicurezza approfondite dei software critici in termini di privacy e di business aziendale, per supportare le aziende nella realizzazione di servizi e prodotti sempre più sicuri.

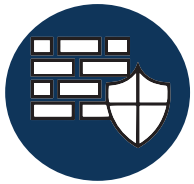
DEFENSE

#INNALZAMENTO DELLE DIFESE #PROGETTAZIONE
DI UN SISTEMA SEMPRE PIÙ SICURO #CULTURA

DEFENSE

COME AUMENTARE LE DIFESE DELLA TUA AZIENDA

SERVIZI PER ELEVARE IL LIVELLO DI SICUREZZA DELLA TUA AZIENDA, ATTRAVERSO STRATEGIE DI PREVENZIONE, DIFESA E FORMAZIONE



BLUE TEAM

Servizi per aiutare le aziende a mettere in essere tutte le misure di difesa necessarie per mitigare e rispondere alle minacce informatiche.

SECURE DESIGN & BUILDING SECURE SOFTWARE

Servizio a supporto delle aziende fin dalla fase iniziale di design di prodotti e servizi, al fine di progettare da subito un sistema che rispetti il requisito “secure by design”.

TRAINING & AWARENESS

Servizi di formazione e informazione, quale elemento chiave per la sicurezza del business, in un ambito in cui il fattore umano è alla base di un’alta percentuale di incidenti informatici, spesso imputabili a mancanza di informazioni e consapevolezza sulle modalità di attacco. I servizi di formazione possono essere rivolti ai diversi ruoli aziendali: management, staff e personale IT.

INCIDENT RESPONSE PLAN

Servizi a supporto delle aziende nell’adeguamento o nella redazione ex-novo di un Piano di Gestione degli Incidenti (IDP).

VERIFICATION

#VULNERABILITY ASSESSMENT
#PENETRATION TEST

VERIFICATION

COME VERIFICARE L'EFFICACIA DELLE SOLUZIONI DI DIFESE DELLA TUA AZIENDA

Verifiche per individuare le vulnerabilità degli asset aziendali: infrastrutture network, sistemi, workstation, mobile, wi-fi, sistemi IoT e applicazioni software e loro codici sorgente. Verifica della sfruttabilità delle vulnerabilità individuate attraverso attività di penetration test.

- VULNERABILITY ASSESSMENT
- PENETRATION TEST APPLICATIVO, DI RETE, DEVICE
- MOBILE SECURITY ASSESSMENT
- SECURE CODE REVIEW

COME IMPLEMENTARE LE REMEDIATION

Servizi di supporto al cliente nell'implementazione delle remediation al fine di ridurre la finestra temporale di esposizione alle vulnerabilità.

ACCREDITED VERIFICATION

#VERIFICHE ACCREDITATE ISO/IEC 17025

ACCREDITED VERIFICATION
PER I SETTORI A PIÙ ALTO RISCHIO

VERIFICHE ACCREDITATE PER CERTIFICARE L'EFFICACIA DEI SISTEMI DI DIFESA

Per ambiti nei quali la sicurezza, la protezione di dati e l'efficacia dei sistemi è fondamentale, vi sono norme e standard internazionali che definiscono i livelli essenziali di sicurezza che specifici prodotti devono rispettare.
Livelli di sicurezza che devono essere verificati da laboratori accreditati secondo la norma ISO/IEC 17025, quali i laboratori del Gruppo IMQ che offrono i seguenti servizi:

Vulnerability Assessment di sistemi (reti e applicazioni) per l'erogazione di servizi fiduciari in ambito eIDAS e nazionale

Valutazioni Formali di Sicurezza secondo i Common Criteria (ISO/IEC 15408) di sistemi e prodotti ICT per la gestione di informazioni classificate e non classificate

Valutazioni della conformità alla IEC 62443 di componenti e sistemi di automazione e controllo in ambito industriale (IACS) e di IACS Service Providers

OPERATIONS

#DETECT #RESPONSE #REMEDIATE

OPERATIONS

COME GESTIRE MINACCE, INCIDENT E REMEDIATION

SERVIZI CONTINUATIVI PER RILEVARE, BLOCCARE E GESTIRE EVENTUALI ATTACCHI INFORMATICI ALLA TUA AZIENDA

Un processo di difesa realmente efficace impone di conoscere nel dettaglio le svariate tecniche di attacco che un'agente offensivo può mettere in campo al fine di raggiungere i propri obiettivi nei confronti di un soggetto attaccato.
Per tale motivo l'approccio del Gruppo IMQ ai servizi continuativi di supporto alla sicurezza in chiave difensiva, si basa e comprende anche un approccio prettamente offensivo.

Detect e Response

Per monitorare l'infrastruttura IT on-premise o Cloud, il traffico di Rete e le anomalie comportamentali (Anomaly Behaviour) degli utenti, con l'obiettivo di identificare un tentativo di attacco o un attacco in corso e reagire tempestivamente prima che questo causi ripercussioni sul business.

Deep & Dark Web Investigation

Per rintracciare nel Web, Dark e Deep Web (con il supporto di strumenti e metodi di ricerca OSINT) informazioni sensibili per l'azienda, quali documenti, credenziali utente o uso improprio del brand.

Early Warning

Per essere avvisati tempestivamente in caso di pubblicazione di una nuova vulnerabilità, potenzialmente rilevante per la propria azienda, e per venire supportati nell'applicazione delle opportune remediation.

Threat Collection and Sharing

Per avere a disposizione un elenco aggiornato degli indicatori di compromissione pubblici, arricchito dalle esperienze sul campo degli specialisti del Gruppo IMQ. Una condivisione delle informazioni quale potente strumento per prevenire un attacco informatico, creando un ecosistema nel quale ognuno sia contemporaneamente contributore e beneficiario.

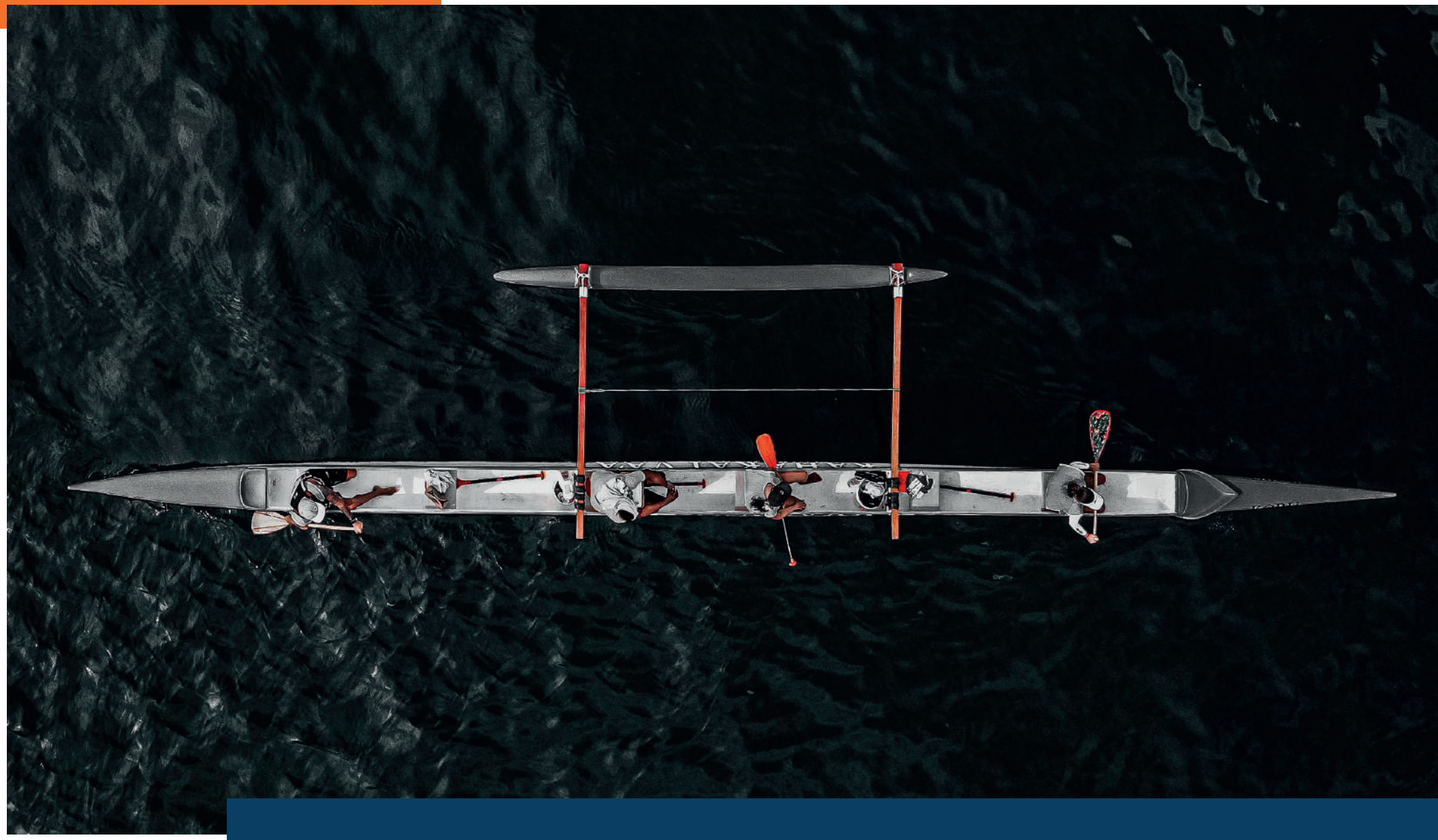
Digital Footprinting

Per mantenere aggiornato il perimetro esposto in termini di indirizzi IP, servizi, applicazioni, così come persone e riferimenti aziendali. Un servizio, utile in particolare alle aziende dall'ampia esposizione Internet o caratterizzate da un forte dinamismo tecnologico.

Incident Response

Per poter contare su un servizio di supporto a seguito di un incidente di sicurezza informatico. Il servizio consiste nell'intervento del Team di specialisti di analisi forense allo scopo di identificare la root cause dell'attacco fino ad arrivare all'eventuale "eradication" del problema.

CERTIFICATION



#ORGANISMO DI CERTIFICAZIONE ACCREDITATO
ISO/IEC 17065, 17021 E 17024

CERTIFICATION
PER OTTIMIZZARE
I SISTEMI DI GESTIONE DELLA SICUREZZA

Nel settore della cyber security ci sono certificazioni obbligatorie e certificazioni volontarie.
Le prime sono richieste per alcuni contesti più critici quali ad esempio la sicurezza militare o la gestione delle identità digitali.
Le seconde, rivolte a tutte le aziende e agli operatori, rappresentano uno strumento per distinguersi sul mercato perché offrono una garanzia visibile di affidabilità e qualità. In alcuni contesti, quali i bandi di gara di grandi realtà, costituiscono un requisito cogente per la partecipazione

CERTIFICAZIONI COGENTI

Certificazione di Trusted Service Providers in ambito eIDAS e nazionale
(Certification & Time Stamping Authorities, Gestori SPID e Conservatori Digitali)

CERTIFICAZIONI VOLONTARIE

SISTEMI DI GESTIONE

ISO/IEC 20000-1 - Certificazione Sistemi di Gestione dei Servizi Informatici
la garanzia di fornire servizi IT di alta qualità

ISO/IEC 27001 - Certificazione Sistemi di Gestione della Sicurezza delle Informazioni
per mantenere i dati al sicuro e darne evidenza a clienti e fornitori

ISO 22301 - Certificazione Sistemi di Gestione per la Continuità Operativa
la garanzia di resilienza organizzativa e capacità di una risposta efficace a un evento critico

CERTIFICAZIONE DELLE FIGURE PROFESSIONALI

SETTORI

SETTORI

- ENERGIA
- PUBBLICA AMMINISTRAZIONE
- MILITARE
- BANCHE FINANZA
- LOGISTICA
- SANITÀ & SALUTE
- AUTOMOTIVE
- TRASPORTI
- UTILITIES
- INDUSTRIA MANIFATTURIERA
- SPORT & TURISMO
- EDILIZIA
- ELETTRONICI
- COMMERCIO
- SERVIZI DIGITALI
- AGRI-FOOD
- HIGH TECH
- NAVALE
- TELECO-MUNICAZIONI
- ASSICURATIVO
- DOMOTICA
- ISTRUZIONE
- CHIMICO FARMACEUTICO
- eIDAS

CREDENZIALI

IMQ È L'UNICA AZIENDA ITALIANA A ESSERE:

LABORATORIO DEDICATO ALLA CYBERSECURITY, ACCREDITATO IN AMBITO "CIVILE" DA OCSI COME LABORATORIO DI VALUTAZIONE FORMALE DELLA SICUREZZA INFORMATICA (LVS) E ACCREDITATO IN AMBITO "MILITARE/GOVERNATIVO" DA DIS/ UCSE COME CENTRO DI VALUTAZIONE DELLA SICUREZZA INFORMATICA (CE.VA.) SECONDO I COMMON CRITERIA (ISO/IEC 15408)

LABORATORIO ACCREDITATO ISO 17025 PER L'EFFETTUAZIONE DELLE PROVE DI VULNERABILITY ASSESSMENT SULLE INFRASTRUTTURE UTILIZZATE PER L'EROGAZIONE DI SERVIZI FIDUCIARI IN AMBITO EIDAS E NAZIONALE

ORGANISMO DI CERTIFICAZIONE ACCREDITATO DA ACCREDIA

- PATENTED TECHNOLOGY & JAVASCRIPT SECURITY
- OWASP CONTRIBUTORS SINCE 2002
- INVITED SPEAKERS AT EUSECWEST, ISACA, ISC2, OWASP, SECURITY SUMMIT, CONFERENCE WORLDWIDE
- TEACHERS AT MASTER IN CYBER SECURITY (BOLOGNA, GENOVA, ROMA TRE UNIVERSITY) AND CYBER CHALLENGE

ELEARN SECURITY WEB APPLICATION PENETRATION TESTER

ELEARN SECURITY WEB APPLICATION PENETRATION TESTER EXTREME

ELEARN SECURITY CERTIFIED PROFESSIONAL PENETRATION TESTER

ELEARN SECURITY MOBILE APPLICATION PENETRATION TESTER

PENTESTER ACADEMY CERTIFIED RED TEAMING EXPERT

EC-COUNCIL CERTIFIED ETHICAL HACKER

PRINCE2® PROJECTS IN CONTROLLED ENVIRONMENTS

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL

OFFENSIVE SECURITY WIRELESS PROFESSIONAL

ISACA CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

EUROPEAN SECURITY ACADEMY OSINT & DARKWEB INVESTIGATIONS

EC-COUNCIL CERTIFIED INCIDENT HANDLER

ISO 27001 LEAD AUDITOR

OSSTMM 3.0 PROFESSIONAL SECURITY TESTER

OSCP EJPT

GIAC GMOB

CSSLP, CISA, CISSP

contattaci: cyber@imqgroup.it

imq.it | intuity.it | mindedsecurity.com

Il Gruppo IMQ è un hub tecnologico per il testing e la certificazione dei requisiti di qualità, sostenibilità, interoperabilità, cybersecurity.

Leader in Europa nella valutazione della conformità (prove, ispezioni, certificazioni), è interlocutore privilegiato dell'industria grazie agli accreditamenti ottenuti e alle specifiche competenze delle società che lo compongono.
Una realtà fatta di tecnici che hanno fatto della qualità, della sicurezza e della sostenibilità l'asse portante del proprio ruolo professionale.

Nell'ambito della cyber sicurezza, grazie al know-how consolidato di IMQ S.p.A. nel settore delle infrastrutture strategiche e in ragione delle recenti acquisizioni (le società IMQ Intuity e IMQ Minded Security con pluriennale esperienza nei servizi a supporto della sicurezza cyber) il Gruppo IMQ si afferma come una realtà unica nel panorama italiano in grado di offrire una visione d'insieme delle problematiche del settore e un approccio olistico alle esigenze del cliente.

Le competenze degli esperti del Gruppo IMQ, attivi e riconosciuti a livello internazionale, consentono di offrire soluzioni sempre aggiornate con le più aggiornate tecniche di test e valutazione.

IMQ Group S.r.l. è la capogruppo del Gruppo IMQ, che è composto da undici Società operative: quattro in Italia - IMQ S.p.A., CSI S.p.A., IMQ Intuity S.r.l. e IMQ Minded Security S.r.l. - e sette all'estero: Spagna (2), Polonia, Turchia, Germania, Emirati Arabi Uniti, Cina.