Emaze Networks

Company Backgrounder

eMaze: i pilastri su cui si fonda

Focus, impegno e lealtà: queste sono le caratteristiche che contraddistinguono Emaze Networks.

Focalizzati per essere il partner di riferimento delle grandi realtà aziendali per la sicurezza informatica.

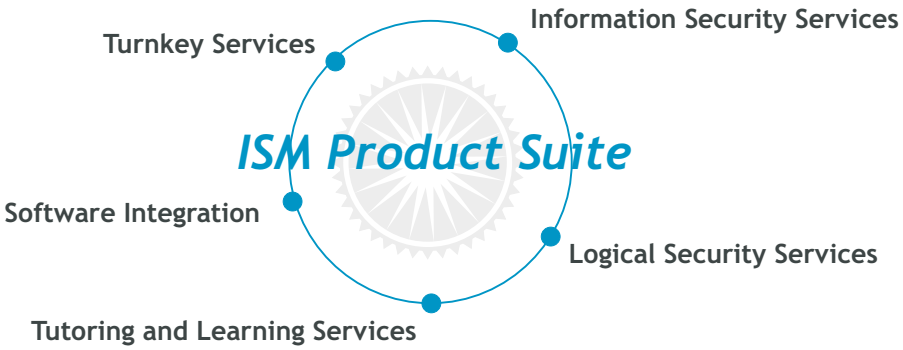
Impegno. Ogni nostro sforzo è diretto a garantire l'integrità e la disponibilità degli asset digitali di valore appartenenti all'azienda nel rispetto del Corporate Business e degli Stakeholder.

Concepiamo la Lealtà come un valore assolutamente fondamentale. **eMaze** garantisce la confidenzialità dell'informazione grazie a una squadra di tecnici accuratamente selezionata e che opera con etica e competenza.

Il campo di azione di eMaze

Il campo d'azione nel quale Emaze è specializzata è l'Informed Security Management nei contesti Enterprise, ovvero l'insieme di processi e infrastrutture di gestione delle vulnerabilità e dei rischi IT per controllare *in continuum* lo stato di sicurezza degli asset digitali.

Il framework di **Informed Security Management (ISM)** è trattato come un processo unitario, ampio e completo in cui progettazione e implementazione portano al raggiungimento della sicurezza nei complessi ambienti ICT e all'allineamento della posizione dell'azienda nei confronti delle norme e degli standard, anche interni.
eMaze offre il proprio supporto a 360 gradi durante la progettazione e implementazione di qualsiasi processo di sicurezza a livello Enterprise al fine di fornire una struttura completa per l'Informed Security aziendale costruita sulle tecnologie di **eMaze**: l' **ISM Product Suite** è di fatto superiore, in quanto a performance e flessibilità, rispetto a qualsiasi prodotto off-the-shelf equivalente sul mercato.



eMaze
informed security

www.emaze.net
info@emaze.net

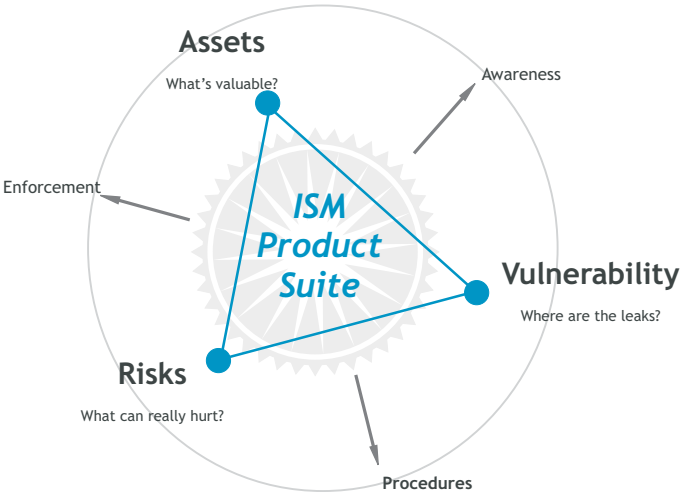
Emaze Networks S.p.A.
reg. imp. Trieste
c.f. - p.iva 00998050322
r.e.a. 116618
cap. soc. € 100.000 i.v.

Sede legale
Area Science Park
ss 14 Km 163,5
loc. Basovizza
I - 34012 Trieste (TS)
tel +39 040 3757580
fax +39 040 3757581

Direzione Generale
Via D. Balestrieri, 6
I - 20154 Milano (MI)
tel +39 02 89078400
fax +39 02 89078420

L'**ISM Product Suite** è il cardine dell'approccio radicale all'Information Security rivolto alle Aziende. L'uso di strumenti e framework generici all'interno dell' Azienda è causa troppo spesso di grandi spese per la sicurezza degli asset meno rilevanti mentre il reale rischio non viene diagnosticato. Questo a causa della grande complessità dei dati elaborati e della mancata individuazione delle relazioni tra i sistemi. Identificare i veri beni informatici di valore è quindi fondamentale.

Ogni campagna di Security condotta da **eMaze** è basata su un minuzioso inventario e una ponderata valutazione degli asset digitali dell'azienda; ne consegue che il Security Assessment è fondamentale nel rendere il Risk Management un input rilevante per la governance dell'Azienda, dando priorità alle applicazioni per la protezione delle risorse strategiche e di maggior valore.



eMaze ISM Product Suite

L'**ISM Product Suite** di **eMaze** è un insieme di metodologie e strumenti indispensabili che ricostruiscono l'esatta correlazione di Asset, Vulnerabilità e Rischi in modo coerente e completo. Questo modello di riferimento è la base di ogni contromisura di Security, incluse le campagne di sensibilizzazione, le misure di Security enforcement e il potenziamento delle procedure aziendali.

ipLegion

IpLegion è la soluzione completa per l'IT Risk e il Vulnerability Management a livello Enterprise.

IpLegion è in grado di individuare gli asset digitali dell'azienda, identifica le minacce e i rischi che affliggono le reti e i sistemi, permette di raccogliere dati riguardanti i rischi e il loro impatto sul business, e, infine, fornisce una visione d'insieme agli Executive e ai Security Manager dell'Azienda, misurando il livello della sicurezza e suggerendo agli amministratori le contromisure più appropriate e monitorando l'effettiva adozione del Remediation plan.

ipLegion ha una architettura distribuita con **Master** (il nucleo centrale di gestione) e **Scout** (le sonde di test) che possono essere virtualizzati. Queste caratteristiche conferiscono alla piattaforma un'eccezionale flessibilità al fine di ottenere una semplifice collocazione e integrazione in ogni struttura ICT complessa e in ogni topologia di network.
La caratteristica che più contraddistingue **ipLegion** è il supporto del partitioning, che consente la suddivisione di tutti gli aspetti tra più contesti totalmente separati tra loro, implementando la soluzione ideale sia per i Managed Security Service Providers (MSSP) che per le grandi corporation aziendali.

ipLegion moduli add-on

ipLegion presenta una architettura modulare con moduli add-on dedicati che lavorano insieme per analizzare e monitorare tutte le possibili minacce. Sono disponibiliI moduli per il rilevamento locale e remoto delle vulnerabilità, con credenziali o senza, per gli attacchi a forza bruta verso password deboli, per la verifica della conformità alle policy ed altro. Ulteriori moduli possono essere progettati e aggiunti sulla base delle specifiche esigenze del Cliente.
Asset Discovery and Management (ADM) è un modulo specifico all'interno della piattaforma **ipLegion**, progettato per individuare in modo passivo i dispositivi conosciuti e sconosciuti, costruendo un inventario completo degli asset digitali e relative vulnerabilità, livelli e fattori di rischio, possibili Remediation plan. Permette agli amministratori il controllo di tutti i dispositivi autorizzati e non autorizzati che appaiono sulla rete aziendale. **ipLegion ADM** è utilizzabile per la verifica automatica dell'osservanza degli standard di sicurezza aziendali di ogni asset digitale, alimentando ed integrando i possibili processi di asset management attivi.
Al fine di affrontare in modo migliore le necessità delle grandi aziende **ipLegion** permette una personalizzazione spinta dove possono essere sviluppati e integrati i “connectors” e i Security Check per le applicazioni custom del cliente. **ipLegion** è la più flessibile piattaforma di Risk and Vulnerability Management presente sul mercato, garantisce una facile integrazione con le tecnologie di cui il cliente è già in possesso e di altre fonti di dati.

Control Room

Control Room è una soluzione di cruscotto per i dati di security innovativa ed altamente efficiente, è modulare ed estremamente flessibile. **Control Room** è stato sviluppato da **eMaze** per sintetizzare tutte le informazioni di sicurezza da ogni fonte e da tutta la rete aziendale.
Sia i dati riguardanti l'infrastruttura che i dati relativi ai processi sono rappresentati in un formato grafico molto intuitivo espressamente ideato per garantire la definizione di strategie preventive e reattive efficaci per tutte le diverse tipologie di asset digitali. **Control Room** combina diversi tipi di dati: da un'intera sede al singolo dispositivo, dalla singola applicazione o processo fino al livello corporate e li mostra da ogni angolazione necessaria. Dall'interfaccia di **Control Room** ogni singolo elemento può essere esaminato in profondità attraverso il Viewer o l'Element Manager.
Control Room ha la capacità di riportare trend storici e associare i dati di Risk management, anche in questo caso con il livello di granularità desiderato, seguendo da vicino l'evoluzione della sicurezza nel tempo.

I servizi offerti da eMaze

Servizi di sicurezza informatica

Grazie alla più efficiente ed efficace combinazione di servizi professionali per i test tecnici (automatici e custom), per i test non tecnici e di assessment e la competenza dei consulenti di sicurezza nella verifica dell'integrità degli asset digitali delle aziende, **eMaze** fornisce alle organizzazioni servizi di consulenza relativi alle Best Practice nell'ambito della security.

Le infrastrutture di information security nuove e già esistenti hanno bisogno di essere testate, valutate e messe in relazione tra loro al fine di raggiungere gli obiettivi dell'azienda in termini di sicurezza informatica. **eMaze** amplia il concetto "classico" di Security Assessment rappresentato da Vulnerabily Assessment (VA) e Penetration Test (PT) includendo attività di progettazione della remediation e supporto per le successive fasi di hardening sia da un punto di vista tecnico che procedurale.

Consapevole della rilevanza per il business delle applicazioni custom e delle problematiche di sicurezza che tipicamente si sviluppano in un'azienda, **eMaze** è in grado di fornire sessioni di Code Inspection e Review su larga scala grazie all'esperienza accumulata dai tecnici nella progettazione software.

All'interno dei progetti delle grandi infrastrutture IT, **eMaze** apporta un valore aggiunto alla scelta della soluzione, favorendo il raggiungimento della sicurezza degli asset di valore dell'Azienda.

Logical security services

Oltre agli aspetti tecnologici, l'Informed Security Management coinvolge processi, procedure, standard e leggi. All'interno dei servizi di Logical Securtiy, **eMaze** è attiva nella progettazione, pianificazione ed esecuzione di ogni fase necessaria al fine di ottenere una piena conformità agli standard di security.

eMaze supporta le imprese sia nel raggiungimento della conformità ai regolamenti locali e alle leggi vigenti (es. Data Protection, SOX)come pure agli standard industriali richiesti o consigliabili(es. PCI-DSS, ISO27001).Inoltre supporta i Clienti nella progettazione e implementazione di tutti i processi di security presenti in un'impresa, con grande attenzione all'attuazione in esercizio della Best Practice corrente. L'approccio per quanto riguarda il Risk Management a livello Enterprise si incentra principalmente sull'enumerazione e la quantificazione del Logical Asset Value che conduce ad una corretta Risk Analisys, la quale a sua volta permette di identificare le priorità delle attività di security nelle aree più esposte al rischio.

Monitorare nel tempo l'efficacia delle misure di sicurezza adottate gioca un ruolo cruciale, **eMaze** è competente per la definizione di KSI (Key Security Indicator) e l'implementazione dei framework di IT Security conformi alle regole generali globalmente accettate a livello Enterprise (es. COBIT).

Servizi chiavi in mano: implementazione SOC

In affiancamento ad ogni Network Operation Center (NOC), la creazione di un Security Operation Center (SOC) è diventata in breve tempo la chiave per garantire la sicurezza ed il mantenimento dei necessari livelli di security. Grazie ad anni di comprovata esperienza nell'implementazione di molti progetti SOC all'interno di grandi imprese, **eMaze** offre, tra le sue attività di core-business, il servizio di implementazione di un SOC chiavi in mano.

Il supporto comprende tutte le fasi dell'implementazione di un SOC, dall'analisi iniziale fino alla verifica. Il progetto, l'implementazione e la messa in opera. Attività che sono condotte tutte rispettando l'assoluta priorità delle procedure e il business del cliente. Una volta che il SOC è attivo può affiancare l'azienda con servizi di SOC Management permettendo al cliente l'outsourcing del monitoraggio, del reporting e dell'attività di controllo.

Software Integration

Il Security coding è un'abilità fondamentale dei programmatori di **eMaze** assieme alla capacità di integrazione dei software, necessarie nel momento in cui si lavora nel panorama di networking all'interno di una grande impresa. Quando la postura di sicurezza dell'impresa richiede degli interventi personalizzati del tipo “glue logic”, **eMaze** sviluppa e consegna soluzioni ad hoc di Security Management. Le referenze in questo campo includono la fornitura di piattaforme di Access Exception Management e strumenti di Automatic Verification, concepiti su misura degli ambienti e dei bisogni dell'azienda interessata.
L'integrazione e la personalizzazione dei prodotti ISM Product Suite all'interno dell'ambiente e con gli strumenti specifici dell'azienda cliente sono il nucleo di tutte le nostre implementazioni: **eMaze** comprende quanto sia importante sfruttare gli investimenti preesistenti e le applicazioni legacy all'interno delle grandi imprese.

Servizi di Formazione e Tutoring

eMaze offre ai suoi clienti servizi di tutoring e di formazione incentrati sulle problematiche di sicurezza aggiornati allo stato dell'arte: le risorse umane sono centrali in ogni processo aziendale di sicurezza.

A seconda delle specifiche esigenze **eMaze** organizza corsi e sessioni di tutoring sia a livello tecnologico che gestionale, in aggiunta alle campagne di sensibilizzazione sul tema della sicurezza dai contenuti più semplici ma di uguale importanza. La combinazione di competenze e l'esperienza dei tecnici permette ad **eMaze** di personalizzare le sessioni di formazione in base alle conoscenze già possedute dai partecipanti, soddisfacendo ogni bisogno di conoscenza dal livello degli Executive Manager fino agli operatori IT.

Gli asset di eMaze

Per lo meno tramite ISM Product Suite, **eMaze** è capace di offrire ai suoi Clienti un prodotto di maggior valore rispetto a qualsiasi altra azienda "classica" di consulenza operante nell'ambito tecnico e gestionale. Grazie alla precisa focalizzazione e alla chiarezza degli obiettivi **eMaze** ha accumulato una grande quantità di asset intangibili sia in termini di proprietà intellettuale che di capitale umano.

eMaze fa saldamente affidamento su piattaforme tecnologiche di sua proprietà, come l'ISM, sviluppata tenendo ben presenti gli specifici bisogni delle grandi aziende: questo permette una notevole superiorità in termini di flessibilità e performance al contrario di ogni altro prodotto mass-market pseudo equivalente.

La proprietà di un set completo di piattaforme software per il Vulnerability Assessment, il Monitoring, il Reporting, l'Asset Inventory, e la Risk Analysis fornisce a **eMaze** una soluzione per il pieno controllo di singoli aspetti da integrare perfettamente negli ambienti del Cliente.

eMaze può contare su diverse metodologie di proprietà studiate per aderire alla perfezione alle necessità dell'azienda: i framework per l'assessment, i Security Measuring Tools (strettamente basati su COBIT) e le metodologie di secure coding. Le metodologie sviluppate vengono tempestivamente aggiornate per tenere conto delle nuove scoperte in materia di gestione della sicurezza.

Lo straordinario valore aggiunto proprio dell'offerta **eMaze** è la grande cura agli aspetti di localizzazione. **eMaze** mantiene un database proprietario delle vulnerabilità opportunamente potenziato per considerare ogni problema per ciascun linguaggio e versione dei sistemi operativi e delle applicazioni.

Dato che ogni cliente opera nel proprio contesto locale **eMaze** segue le normative di legge per garantire la maggiore aderenza possibile agli obblighi di sicurezza.

Le conoscenze sono l'asset di maggior valore per **eMaze**; la combinazione di competenze peculiari dei membri dello staff tecnico e manageriale garantisce la completa copertura su ogni specifico aspetto della sicurezza ed ha l'abilità di riportare e condividere i concetti base con le figure corporate.

Le persone di eMaze

Il successo di **eMaze** per gran parte dipende dal continuo investimento nella selezione, nel potenziamento, nella formazione e nella motivazione delle risorse umane.

Il dipartimento di ricerca e sviluppo si trova all'interno di uno dei più prestigiosi centri di ricerca italiani: questa è una scelta strategica che rende possibile l'osmosi tra conoscenze di ambito accademico e industriale.

I tecnici hanno un'esperienza sopra la media nel campo della Sicurezza Informatica (oltre 8 anni), molti di loro sono noti nel settore grazie a pubblicazioni e seminari, e vengono considerati degli Industry Guru.

In aggiunta, con le risorse umane, **eMaze** adotta una policy etica molto stringente, con l'obiettivo di creare una forte identificazione del personale con l'azienda e la sua missione, per garantire lealtà ai Clienti in qualità di Security partner .

Il personale di **eMaze** ha ottenuto le certificazioni più prestigiose, tra le altre: ISO27001 (Lead Auditor), ITIL/ISO IEC 20000, CISA (Certified Information Security Auditor), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), GCIH (GIAC Certified Incident Handler). Emaze è certificata Novell Sentinel Partner.

eMaze: la presenza

eMaze ha scelto tre località italiane strategiche come sedi principali per i propri uffici. Roma e Milano, per essere in contatto con i più importanti centri d'affari, e Trieste, presso l'Area Science Park, per stare all'interno di uno dei poli di ricerca italiani più innovativi.